# Audit
# Report

FOREIGN NATIONAL SECURITY CONTROLS
AT DOD RESEARCH LABORATORIES

Report No. D-2001-007

October 27, 2000

## Office of the Inspector General
## Department of Defense

DTIC QUALITY INSPECTED 4

20001102 022

AQI 01-01- 0165

**Acronyms**

| | |
|---|---|
| DARPA | Defense Advanced Research Projects Agency |
| NDP-1 | National Disclosure Policy-1 |
| NISPOM | National Industrial Security Program Operating Manual |

October 27, 2000

MEMORANDUM FOR DIRECTOR, DEFENSE ADVANCED RESEARCH PROJECTS
AGENCY
NAVAL INSPECTOR GENERAL

SUBJECT:  Audit Report on Foreign National Security Controls at DoD Research
Laboratories (Report No. D-2001-007)

We are providing this report for your information and use.  We conducted the audit
in response to Public Law 106-65, National Defense Authorization Act for Fiscal Year
2000, section 1402, "Annual Report on Transfer of Militarily Sensitive Technologies to
Countries and Entities of Concern."  We considered management comments on a draft of
this report in preparing the final report.

The Department of the Navy and Defense Advanced Research Projects Agency
comments conformed to the requirements of DoD Directive 7650.3 and left no unresolved
issues.  No additional comments are required.

We appreciate the courtesies extended to the audit staff.  For additional information
on this report, please contact Ms. Evelyn R. Klemstine at (703) 604-9172 (DSN 664-9172)
or Mr. Timothy E. Moore at (703) 604-9633 (DSN 664-9633).  See Appendix E for the
report distribution.  The audit team members are listed inside the back cover.

Robert J. Lieberman
Assistant Inspector General
for Auditing

**Office of the Inspector General, DoD**

Report No. D-2001-007                                    October 27, 2000
(Project No. D1999LG-0034.03)

# Foreign National Security Controls
# at DoD Research Laboratories

## Executive Summary

**Introduction.** Public Law 106-65, National Defense Authorization Act for Fiscal Year 2000, section 1402, "Annual Report on Transfer of Militarily Sensitive Technologies to Countries and Entities of Concern," requires an annual interagency review on the transfer of militarily sensitive technologies to countries and entities of concern. We visited the Defense Advanced Research Projects Agency in Arlington, Virginia; the Army Research Laboratory in Adelphi, Maryland; the Naval Research Laboratory in Washington D.C.; and the Air Force Research Laboratory-Munitions at Eglin Air Force Base, Florida. From October 1, 1998, through December 31, 1999, those four sites had 2,337 foreign visitors, of which 873 were official visits originating from the foreign visitors' embassies.

**Objectives.** The overall audit objective was to evaluate the adequacy of DoD policies and procedures to prevent the transfer of technologies and technical information with potential military application to countries and entities of concern. This is the fourth in a series of reports on that issue. Report No. D-2000-110, "Export Licensing at DoD Research Facilities," March 24, 2000, addresses the DoD portion of the required FY 2000 export licensing interagency review at DoD research facilities. Report No. D-2000-109, "Interagency Review of the Export Licensing Process for Foreign National Visitors," March 2000, was an interagency review of Federal agencies' compliance with the deemed export licensing requirements contained in the Export Administration Regulations and the International Traffic in Arms Regulations. Report No. D-2000-130, "Foreign National Access to Automated Information Systems," May 26, 2000, addresses whether automated information system access controls and physical security controls for foreign national visitors were adequate at research facilities owned or sponsored by DoD. For this report, we determined whether foreign disclosure instructions[*] were prepared when required and whether information disclosure restraints were disseminated to all relevant individuals and organizations interacting with foreign nationals. We also reviewed management control programs related to our objective.

**Results.** The dissemination of foreign disclosure instructions at the Army Research Laboratory and the Air Force Research Laboratory-Munitions provided reasonable assurance that release of controlled unclassified and classified information to foreign nationals was in accordance with visit authorizations or certifications. However, the Defense Advanced Research Projects Agency and the Naval Research Laboratory controls over the dissemination of foreign disclosure instructions needed improvement. Specifically, for 208 of 270 official visits reviewed, the Defense Advanced Research

---

[*]Includes visit authorization letters and delegation of disclosure authority letters.

Projects Agency and the Naval Research Laboratory did not disseminate foreign disclosure instructions to the program managers hosting foreign nationals. As a result, the Defense Advanced Research Projects Agency and the Naval Research Laboratory program managers were hosting foreign nationals on official visits unaware of national security foreign disclosure restraints and may have inadvertently released unauthorized technical information to other countries (finding A).

The Military Department laboratories' approval processes for visits by foreign nationals were adequate (see Appendix C). However, the Defense Advanced Research Projects Agency security controls over the approval process for foreign national visitors were weak. Specifically, controls for granting building access for foreign national visitors representing U.S. entities required improvement. Also, the Defense Advanced Research Projects Agency database contained inconsistent and inaccurate data. As a result, controls over the disclosure of controlled unclassified information to foreign nationals were not effective and the Defense Advanced Research Projects Agency may have inadvertently disclosed controlled unclassified information to other countries, including countries of concern, without authorization (finding B).

See Appendix A for details on our review of the management control program.

**Summary of Recommendations.** We recommend the Director, Defense Advanced Research Projects Agency, and the Commanding Officer, Naval Research Laboratory, develop local procedures to ensure foreign disclosure instructions from foreign visit approval authorities are disseminated to the program managers hosting foreign nationals. We recommend that the Director, Navy International Programs Office, revise applicable guidance to ensure foreign disclosure restrictions contained in visit authorization letters to the proposed hosts of the visit are disseminated. We recommend the Director, Defense Advanced Research Projects Agency, enforce and improve security procedures to ensure visits by foreign nationals are sufficiently documented. We also recommend the Director, Defense Advanced Research Projects Agency, prepare a manual providing specific procedures for the preparation of Visitor Control Center records and develop input methods to ensure the Defense Intelligence Agency visit approval letter is used as the primary source document for all information regarding official foreign national visitors.

**Management Comments.** The Director, Defense Advanced Research Projects Agency, concurred with the recommendations, stating corrective actions have begun. The Office of the Assistant Secretary of the Navy (Research, Development and Acquisition) concurred with the finding and recommendations, stating that all notification letters will require dissemination of disclosure restrictions to visit hosts. A discussion of management comments is in the Findings section of the report and the complete text is in the Management Comments section.

# Table of Contents

# Background

Public Law 106-65, National Defense Authorization Act for Fiscal Year 2000, section 1402, "Annual Report on Transfer of Militarily Sensitive Technologies to Countries and Entities of Concern," October 5, 1999, requires that the Inspectors General of the Departments of Commerce, Defense, Energy, and State, in consultation with the Director, Central Intelligence Agency, and the Director of the Federal Bureau of Investigation, conduct annual reviews of the transfer of militarily sensitive technologies to countries and entities of concern. Report No. D-2000-110, "Export Licensing at DoD Research Facilities," March 24, 2000, addresses the DoD portion of the required FY 2000 export licensing interagency review. Report No. D-2000-130, "Foreign National Access to Automated Information Systems," May 26, 2000, addresses foreign national access to automated information systems and physical security controls. This report expands the areas reviewed in Report No. D-2000-110 and addresses security controls for foreign nationals visiting DoD research laboratories.

Foreign nationals visit DoD research laboratories under various international agreements and programs. Technical data at DoD research laboratories can be released to a foreign national during a short-term visit or during the period of the foreign visitor's assignment through either the individual's integration into the installation work force as an extended visitor or through the individual's specific request for release of technical information or documentation. National Disclosure Policy-1, "National Policy and Procedures for the Disclosure of Classified Military Information to Foreign Governments and International Organizations,"(NDP-1) October 1, 1988, prescribes requirements for the disclosure of classified military information to foreign governments. The requirements for the release of controlled unclassified information[1] and classified information to foreign nationals working in or visiting DoD research laboratories is prescribed by DoD Directive 5230.20, "Visits, Assignments, and Exchanges of Foreign Nationals," August 12, 1998 (DoDD 5230.20), for a visit sponsored by the foreign visitor's government. DoD Manual 5220.22-M, "National Industrial Security Program Operating Manual," (NISPOM) January 1995, prescribes requirements for the release of classified information to foreign nationals who represent a U.S. company or a U.S. academic institution.

**The NDP-1.** The NDP-1 states that before any discussions with foreign representatives on the negotiation of an international agreement, DoD Components will determine the extent to which classified military information will be required for release and will obtain disclosure authorization for the information. The disclosure planning will include the preparation of a delegation of disclosure authority letter to be used to provide guidance to subordinate commands and agencies, and, when applicable, to DoD contractors.

---

[1]Controlled unclassified information is unclassified information to which access or distribution limitations have been applied in accordance with national laws, policies, or regulations.

**Foreign Disclosure Requirements.** Foreign disclosure directives and policies require that a delegation of disclosure authority letter be prepared for foreign nationals involved in the Cooperative Program Personnel, Defense Personnel Exchange Program, or Foreign Liaison Officer arrangement. Delegation of disclosure authority letters must also be prepared before any negotiations for an international agreement begins; therefore, a delegation of disclosure authority letter must exist for all meetings related to international agreements. Visits by foreign nationals representing foreign entities, either foreign governments or foreign-controlled corporations, must be arranged through the applicable embassy. Visits by foreign nationals representing U.S. entities, either U.S. contractors or U.S. academic institutions, are generally restricted to unclassified meetings and only information in the public domain may be released to the foreign nationals unless they have export licenses.

DoDD 5230.20 states that a delegation of disclosure authority letter, or equivalent written disclosure guidance, approved by the appropriate designated disclosure authority, will be provided to the contact officer for foreign nationals who are assigned at a DoD Component under a Cooperative Program Personnel, Defense Personnel Exchange Program, or Foreign Liaison Officer arrangement. Information approved for disclosure to foreign nationals who visit a DoD Component under a visit authorization will be described in the applicable visit authorization letter or certification.

**Approval Authority for Foreign Nationals Representing Foreign Entities.** For official visits, that is, for meetings that involve foreign nationals representing foreign entities,[2] a designated disclosure authority must approve foreign disclosure. The approval is documented in a visit authorization letter signed by a foreign disclosure officer. If a delegation of disclosure authority letter is applicable to the purpose of the proposed meeting, the foreign disclosure officer will reference the delegation of disclosure authority letter in foreign disclosure instructions contained in the visit authorization letter. For the Defense Advanced Research Projects Agency (DARPA) in Arlington, Virginia, foreign disclosure authorization is centralized within the Director's office. For the Army Research Laboratory (the Army Lab) in Adelphi, Maryland, foreign disclosure is approved by command-assigned foreign disclosure officers. For the Naval Research Laboratory (the Navy Lab) in Washington, D.C., foreign disclosure authorization is centralized within the Navy International Programs Office; however, there are command-assigned foreign disclosure officers for specific international agreements. For the Air Force Research Laboratory-Munitions (the Air Force Munitions Lab) at Eglin Air Force Base, Florida, foreign disclosure is approved by command-assigned foreign disclosure officers.

---

[2]Foreign entities, as used in this report, refers to foreign governments and foreign-controlled corporations.

**Approval Authority for Foreign Nationals Representing
U.S. Entities.**[3] For all visits by foreign nationals, the NISPOM requires a visit
request so that hosting commands can make administrative arrangements, obtain
security assurances, and develop disclosure decisions. The visit request
identifies the visitors, specifies the dates and purpose of the visit, and provides
the visitor's citizenship, place of birth, and security clearance. However, the
NISPOM only covers the disclosure of classified information and
export-controlled technical data. The DoD guidance on disclosure of controlled
unclassified information is primarily contained in DoDD 5230.20 and DoD
Directive 5230.25, "Withholding of Unclassified Technical Data from Public
Release," November 6, 1984. DARPA did not require visit requests from
foreign nationals representing U.S. entities (unofficial visits) unless the
proposed meeting was expected to be classified. The Military laboratories
required visit requests for all visits.

Table 1 shows the approval authorities required for each type of visit at the
commands we reviewed.

| Table 1. Approval Authority | | | | |
|---|---|---|---|---|
| Foreign National | DARPA | Army Lab | Navy Lab | Air Force Munitions Lab |
| Representing foreign entities | Director[1] | FDO[2] | NIPO[3] | FDO[2] |
| Representing U.S. entities | | | | |
|   One-time | Pgm Mgr[4] | FDO[2] | Superintendent[5] | FDO[2] |
|   Recurring | Pgm Mgr[4] | Director[6] | Superintendent[5] | FDO[2] |
|   Extended | Pgm Mgr[4] | Director[6] | CO/DoR[7] | FDO[2] |

[1] DARPA director
[2] Foreign disclosure officer (command-assigned)
[3] Navy International Programs Office
[4] Program manager
[5] Navy Lab division superintendent
[6] Army Lab director
[7] Navy Lab commanding officer or director of research

---

[3]U.S. entities, as used in this report, refers to U.S. corporations and U.S. academic institutions.

# Objectives

The overall objective was to evaluate the adequacy of DoD policies and procedures to prevent the transfer of technologies and technical information with potential military application to countries and entities of concern. Specifically, we determined whether foreign disclosure instructions, including visit authorization letters and delegation of disclosure authority letters, were prepared when required and whether information disclosure restraints were disseminated to all relevant individuals and organizations interacting with foreign nationals. We also reviewed management control programs at the research laboratories related to the specific objective. See Appendix A for a discussion of the scope and methodology and our review of the management control program. See Appendix B for prior coverage related to the objectives.

# A. Dissemination of Foreign Disclosure Instructions

The dissemination of foreign disclosure instructions at the Army Lab and the Air Force Munitions Lab provided reasonable assurance that release of controlled unclassified and classified information to foreign nationals was in accordance with visit authorization and delegation of disclosure authority letters. However, DARPA and Navy Lab controls over the dissemination of foreign disclosure instructions needed improvement. Specifically, for 208 of 270 official visits reviewed, DARPA and the Navy Lab did not disseminate foreign disclosure instructions to the program managers hosting foreign nationals because DARPA and Navy instructions did not clearly state the procedures to be used for the dissemination of foreign disclosure instructions. As a result, DARPA and the Navy Lab program managers were hosting foreign nationals on official visits unaware of national security foreign disclosure restraints that pertained to the visitor's country of origin. Therefore, DARPA and the Navy Lab may have inadvertently released unauthorized technical information to other countries.

## Foreign Disclosure Policies

**DoDD 5230.20.** DoDD 5230.20 provides overall DoD guidance for foreign national visits. The directive establishes and describes the process for visits of foreign nationals to DoD Components over which the DoD Components have security responsibility. DoDD 5230.20 describes and is applicable to three types of foreign national visit authorizations:

- one-time, for a specified purpose (normally less than 30 days);

- recurring, for approved agreements, contracts, licenses, or programs (annual revalidation and review are required); and

- extended, for assignments under Cooperative Program Personnel, Defense Personnel Exchange Program, or Foreign Liaison Officer arrangement.

The directive states that DoD Components supported by the Defense Intelligence Agency will obtain a disclosure authorization from the originating department or agency for the release of any controlled unclassified or classified information that is not under the DoD Components' disclosure jurisdiction. It further states that DoD Components will notify the Defense Intelligence Agency Foreign Liaison Office when they extend invitations to foreign nationals for a hosted visit to their organization so that the Defense Intelligence Agency can obtain the necessary security assurances in advance of the visit.

DoDD 5230.20 states that foreign nationals will be provided access only to that controlled unclassified and classified information that has been authorized for release to their government. DoDD 5230.20 does not apply to foreign national

5

employees of U.S. corporations owned by foreign interests or to foreign nationals who are not representing their government in an official capacity.

**The Advanced Research Projects Agency Security Manual.** "The Advanced Research Projects Agency Security Manual" (the DARPA Security Manual), December 10, 1990, establishes a system for classifying, downgrading, and declassifying information; sets forth policies and procedures to safeguard such information; and provides for oversight and administrative sanctions for violations. Regarding access by visitors, whether foreign nationals or U.S. citizens, the security manual is explicit. The manual states that non-DARPA individuals must have their security clearances and visit requests sent to the DARPA Visitor Control Center at least 2 weeks in advance of an intended visit. Visit requests normally should include:

- full name, date and place of birth, social security number, and rank or grade of visitor;

- security clearance of the visitor;

- employer of the visitor;

- name and address of the organization to be visited;

- dates and duration of proposed visits;

- purpose of visit in sufficient detail to establish need-to-know; and

- name of person at DARPA to be contacted for visit verification.

**DARPA Standard Operating Procedures for Foreign Visitors.** DARPA had informal standard operating procedures for processing visits by foreign nationals. Separate procedures existed for official visitors and non-official[4] visitors.

**Official Visitor Standard Operating Procedures.** An official foreign national visitor is any non-U.S. citizen who represents a foreign nation or a business incorporated in a foreign nation. Regardless of the classification level of the proposed meeting, official foreign national visitors are required to submit visit requests through their embassy. The visit request is routed through the Defense Intelligence Agency for verification of information before it comes to DARPA for approval. The DARPA Security and Intelligence Directorate reviews the visit request and forwards it to the sponsoring DARPA program manager for a recommendation of approval or disapproval. The Security and Intelligence Directorate then notifies the Defense Intelligence Agency of the program manager's recommendation. When the visit approval letter is received from the Defense Intelligence Agency, the DARPA Security and Intelligence Directorate reviews the letter for disclosure issues and, if necessary, reviews those issues with the program manager hosting the visit. The Security and

---

[4]DARPA usage of the term "non-official visitor" should not be confused with its usage of the term "unofficial visitors."

Intelligence Directorate keeps a file for each official visit. The process generally takes 30 days; however, if necessary, it can be done much faster.

**DARPA Non-Official Visitor Standard Operating Procedures.** A non-official visitor is any non-U.S. citizen who is an immigrant alien, or a non-immigrant alien who represents a U.S. contractor or contracted U.S. academic institution. Non-official visitors do not need to give prior notification to DARPA if they intend to visit a DARPA employee.

Foreign nationals or immigrant alien employees representing U.S. entities do not need to submit visit requests. Only unclassified, non-sensitive information can be shared with those visitors. The only exceptions are if the U.S. employer provides the foreign national or immigrant alien a copy of an approved export license for the information or provides some other form of documentation that explains the information and classification levels that can be disclosed to the foreign national.

Foreign nationals or immigrant aliens who are visiting a DARPA employee for personal reasons and discussions are considered unofficial visitors. They are not required to submit official visit requests. Their discussions are limited to DARPA information that is approved for public release.

**Navy Guidance.** Secretary of the Navy Instruction 5510.34, "Manual for the Disclosure of Department of the Navy Military Information to Foreign Governments and International Organizations," November 4, 1993, provides Navy policy and procedures for the disclosure of controlled unclassified and classified military information to foreign governments and international organizations. It states that visits by foreign representatives must be controlled to ensure that the visitors receive access to only controlled unclassified and classified information that is authorized by a designated disclosure official for disclosure to the foreign government. With some exceptions, foreign requests for official visits to Navy commands, organizations, and contractor facilities will be submitted by the applicable embassy to the Navy International Programs Office. The Navy International Programs Office, or other approving authority, will provide a disclosure authorization, with restrictions as necessary, to the security officer of the Government facility being visited. The disclosure authorization is valid only for the individuals named in the request, for the period of time specified, and for the stated purpose of the visit. Discussions of subjects not included in the disclosure authorization are prohibited.

# Disclosure of Information to Foreign Nationals

Controls at the Army Lab and the Air Force Munitions Lab provided reasonable assurance that release of controlled unclassified and classified information to foreign nationals was in accordance with applicable visit authorizations or certifications. DARPA and Navy Lab security controls over the disclosure of information to foreign nationals representing foreign entities needed strengthening. From October 1, 1998, through December 31, 1999, those four sites had 2,337 foreign visitors, of which 873 were official visits originating from the foreign visitors' embassies.

7

At DARPA and each of the Military laboratories, we verified whether visit authorizations signed by foreign disclosure officers existed and whether foreign disclosure instructions contained in the visit authorization letters were disseminated for all visits by foreign nationals representing foreign entities. Our review disclosed that the Army Lab and Air Force Munitions Lab disseminated foreign disclosure information to the hosts of the foreign visitors; however, DARPA and the Navy Lab many times did not. It is important that foreign disclosure instructions be disseminated because the foreign disclosure instructions in visit authorization letters refer to specific documents, such as delegation of disclosure authority letters, and are specific according to the country of the foreign national and the international agreement related to the purpose of the visit. Although the program manager hosting the foreign national is clearly the individual for whom the information is intended, many times the foreign disclosure instructions were not disseminated past the security office of the organization being visited.

**The Army Lab and the Air Force Munitions Lab.** The Army Lab and the Air Force Munitions Lab had procedures to ensure that foreign disclosure instructions were provided to the visit points of contact for all visits.

    **The Army Lab.** We interviewed 16 Army Lab visit points of contact to determine whether the Intelligence and Security Office had briefed foreign disclosure instructions to them. Each stated that they had been briefed on foreign disclosure instructions and were aware that current Army Lab policy limits the disclosure of information to unclassified, public domain information, unless a data exchange agreement, delegation of disclosure authority letter, or program agreement exists. If questions or concerns arose, each felt comfortable asking help from the Intelligence and Security Office.

    **The Air Force Munitions Lab.** Through interviews with Air Armament Center foreign disclosure personnel and Air Force Munitions Lab security personnel, in addition to analysis of procedures, we verified that foreign disclosure instructions had been briefed to the hosts of the foreign national visitors. We also interviewed 14 Air Force Munitions Lab visit points of contact to determine whether they had received foreign disclosure instructions from the Air Armament Center foreign disclosure personnel. Each stated that they had received foreign disclosure instructions as necessary before meetings took place.

**DARPA and the Navy Lab.** DARPA did not provide foreign disclosure instructions from the Defense Intelligence Agency to the visit points of contact for about 60 percent of visits reviewed. The Navy Lab did not provide foreign disclosure instructions from the Navy International Programs Office to the visit points of contact for about 82 percent of visits reviewed.

Table 2 shows the results of our review.

| Table 2.  Results of Foreign Disclosure Review (Official Visits) | | | |
|---|---|---|---|
| Laboratory Reviewed | No. of Records Reviewed | No. of Visit Authorizations | No. Notified |
| DARPA | 57 | 51 | 23 |
| Army Lab | 20 | 20 | 20 |
| Navy Lab | 213 | 196 | 39 |
| Air Force Munitions Lab | 410 | 410 | 410 |

## Foreign Disclosure at DARPA and the Navy Lab

DARPA and the Navy Lab did not disseminate foreign disclosure instructions to program managers hosting foreign national visitors representing foreign entities because DARPA and Navy instructions do not clearly state the procedures to be used for the dissemination of foreign disclosure instructions.

**Foreign Disclosure at DARPA.** The DARPA record of foreign visits was contained in the Security Information Management System database. The database had records of 660 visits by foreign nationals from October 1, 1998, through December 31, 1999, a period of 15 months. Of the 660 visits, 596 were visits by foreign nationals representing U.S. entities. The other 64 visits were by foreign nationals representing foreign entities.

For more than half of the visits by foreign nationals representing foreign entities that we reviewed, the DARPA Security and Intelligence Directorate did not disseminate foreign disclosure instructions received from the Defense Intelligence Agency to the program managers hosting foreign national visitors. By reviewing the Security and Intelligence Directorate records of each visit by a foreign national representing a foreign entity, we determined that DARPA did not provide instructions to the visitor's host for 34 of 57 visits. The Defense Intelligence Agency faxes those instructions, included in the visit authorization letter, to the DARPA Security and Intelligence Directorate. However, that office did not disseminate the information in all instances. When foreign disclosure instructions were provided to the point of contact, they were sent by

the Security and Intelligence Directorate through electronic mail to the program manager hosting the visit, a process that effectively disseminated the instructions.

**Official Visits by Foreign Nationals Representing Foreign Entities.** For 34 of 57 visits by foreign nationals representing foreign entities, DARPA did not provide foreign disclosure instructions to the foreign visitor's host. The DARPA Security Manual does not provide policy or procedures for the dissemination of foreign disclosure limitations to the program managers who interact with or host visitors. The DARPA Security and Intelligence Directorate informal standard operating procedures for foreign visitors state that the Security and Intelligence Directorate will review the visit approval for disclosure issues and, if necessary, will review those issues with the program manager prior to the visit. However, since November 1999, a GS-13 Security Specialist position with supervisory duties over foreign disclosure duties had been vacant. As of June 2000, the position was still vacant. Contract personnel performing foreign disclosure duties were performing those duties under the supervision and control of the Security and Intelligence Director in accordance with procedures listed in the standard operating procedures, but the standard operating procedures do not provide guidance on when program manager reviews are necessary or provide specific procedures for reviewing foreign disclosure issues with program managers prior to visits. The contract personnel had begun sending foreign disclosure instructions to program managers by electronic mail in some cases, but, in a majority of cases, there was no contact with program managers after visits were approved.

**Unofficial Visits by Foreign Nationals Representing U.S. Entities.** We selected a judgmental sample of 12 visits by foreign nationals representing U.S. entities from the Security Information Management System database. We selected visits by foreign nationals from countries of concern[5] and visits by foreign nationals to discuss targeted technologies[6] as identified by the Defense Security Service. For each of those selected visits, we interviewed the point of contact identified in the database. We verified that the visit took place, the dates of the visit, the information that was discussed, and what information had been released to the foreign nationals. Because DARPA did not require advance notice of unofficial visits (as discussed in finding B), foreign disclosure instructions were not prepared or disseminated to the program managers who interacted with or hosted the foreign national visitors.

**Foreign Disclosure at the Navy Lab.** The Navy Lab record of foreign visits was kept in a database developed by the head of security in the Command Support Division. The Foreign Visits database had records of 952 visits by foreign nationals from October 1, 1998, through December 31, 1999, a period

---

[5]For this audit, countries of concern were taken from a list compiled by the Department of Energy for reasons of national security, nonproliferation, anti-terrorism, or economic security.

[6]The Defense Security Service defines targeted technologies as aeronautics systems, armaments and energetic materials, electronics, information systems, sensors and lasers, and signature control.

of 15 months. Of the 952 visits, 739 were visits by foreign nationals representing U.S. entities. The other 213 visits were by foreign nationals representing foreign entities.

The Navy Lab did not disseminate foreign disclosure instructions from its security office to the program managers hosting foreign national visitors representing foreign entities. Secretary of the Navy Instruction 5510.34 states that approving authorities will provide disclosure authorization, with restrictions as necessary, to the security officer of the Government facility being visited, but it does not require the facility to disseminate the restrictions to the proposed hosts of the visit. The Navy Lab Memorandum, "Visits to NRL [Naval Research Laboratory] by Foreign Nationals," July 27, 1999, states that "people the visitor(s) will interact with must be aware of their foreign status and thoroughly familiar with disclosure limitations," but does not provide procedures for ensuring the people the visitors will interact with will be familiar with the disclosure limitations.

**Official Visits by Foreign Nationals Representing Foreign Entities.** The Navy Lab security office for 174 of 213 visits did not disseminate foreign disclosure instructions contained in visit authorization letters to the Navy Lab program managers hosting the foreign visitors. Those instructions were faxed by the Navy International Programs Office to the Navy Lab security office in accordance with Navy regulations; however, the security office did not disseminate the information. Through an analysis of the Navy Lab foreign disclosure procedures and regulations, we determined that there were no official procedures for dissemination of foreign disclosure instructions. The head of the security office and five program managers who had hosted official visits confirmed that instructions were not disseminated to program managers. The Navy Lab security head stated that he viewed the dissemination of foreign disclosure instructions to program managers as a foreign disclosure function, not a security office function. Of the 213 official visits to the Navy Lab that we reviewed, there were 39 instances where Navy Lab personnel with foreign disclosure authority approved visits. In those instances, further dissemination of foreign disclosure instructions was unnecessary as the authorized foreign disclosure officers were hosting the visits.

**Unofficial Visits by Foreign Nationals Representing U.S. Entities.** The controls in place at the Navy Lab over foreign disclosure appear to provide reasonable assurance that information was being properly released to foreign nationals representing U.S. entities (unofficial visits). We selected a judgmental sample of 17 visits by foreign nationals representing U.S. entities from the Foreign Visits database. We selected visits by foreign nationals from countries of concern and visits by foreign nationals to discuss targeted technologies. For each of those visits, we interviewed the point of contact identified in the Foreign Visits database. We verified that the visit took place, the dates of the visit, the information that was discussed, and what information had been released to the foreign nationals.

# Effect of Foreign Disclosure Control Weaknesses

DARPA may have inadvertently disclosed controlled unclassified information to foreign nationals without authorization. The Navy Lab may have inadvertently disclosed controlled unclassified and classified information to foreign nationals without authorization. Information on developing technologies available at DARPA and the Navy Lab is highly sensitive. DARPA develops imaginative, high-risk research ideas that offer significant technological impact. DARPA pursues technological concepts from the demonstration of technical feasibility through the development of prototype systems. The Navy Lab serves as the Navy's corporate laboratory and conducts programs of scientific research and advanced technological development directed toward maritime applications of atmospheric, ocean, and space sciences. The Navy Lab researches materials, new and improved equipment, systems, and techniques that relate to maritime applications.

The following situations illustrate the effect of not disseminating foreign disclosure instructions to hosts of foreign nationals.

- On October 18 and 19, 1999, a Greek commander and lieutenant commander, representing the Hellenic Navy General Staff, met with the Navy Lab to discuss electronic warfare. The visit hosts requested that the meeting be approved at the NATO Secret security clearance level. The Navy International Programs Office approved the meeting at the Unclassified security clearance level. There was no evidence that the visit hosts had been informed that a lower level of clearance than they had requested had been approved. There was also no evidence related to the actual visit that proved whether discussions were held at the NATO Secret level.

- On September 7, 1999, a group of Australian scientists, representing the Australian Defence Science and Technology Organisation, visited the Navy Lab to discuss a collaborative research and development project. The visit hosts requested that the meeting be approved at the Top Secret security clearance level. The Navy International Programs Office approved the meeting at the Secret security clearance level. There was no evidence that the visit hosts had been informed that a lower level of clearance than they had requested had been approved. We could not determine from the documentation whether Top Secret information had been discussed.

- From July through December 1999, a Royal Australian Navy lieutenant commander had approval for recurring visits to the Navy Lab to discuss countermeasures for anti-ship missiles. The visit hosts requested that the meetings be approved at the Top Secret security clearance level. The Navy International Programs Office approved the meetings at the Secret security clearance level. There was no evidence that the visit hosts had been informed that a lower level of

12

clearance than they had requested had been approved. We could not determine from the documentation whether Top Secret information had been discussed.

- In July 1999, a United Kingdom civilian, representing the United Kingdom Defence Engineering and Research Agency, flew aboard a Navy Lab P-3 aircraft as an observer. Explicit foreign disclosure instructions included that the visitor was authorized as a passenger only to observe tests and act as an advisor; that the aircraft would be configured with authorized research and development software; and that no device to test, measure, or record U.S. systems, or audio visual equipment, computers, or communication equipment, including cellular telephones, could be brought aboard. There was no evidence that those instructions had been presented to the visit hosts.

- On April 9, 1999, a French engineer, representing a French company, visited the Navy Lab to attend a meeting discussing experiments on microelectronics for space applications. The visit hosts requested that the visit be approved at the Unclassified security clearance level. The visit was approved at less than the Unclassified security clearance level. The visit authorization letter was very explicit: "THIS VISIT MUST BE PUBLIC DOMAIN INFORMATION ONLY." There was no evidence that the visit authorization letter had been provided to the visit hosts.

As the above situations illustrate, visit authorization letters provide important foreign disclosure instructions. Strong foreign disclosure controls require that the program managers who host visits by foreign nationals representing foreign entities must be informed of the foreign disclosure instructions that are contained in visit authorization letters. Awareness of the foreign disclosure instructions ensures hosts do not inadvertently release technical information to countries not authorized to receive it.

## Management Comments on the Finding and Audit Response

**DARPA Comments.** DARPA believes its security education program and the information available on its intranet web site provide appropriate information and instructions to the visit hosts. DARPA requested that the Inspector General, DoD, accept that DARPA procedures for visitor control and notification of hosts, when coupled with the DARPA default – that in the absence of specific disclosure instructions, hosts are to disclose only publicly released information – are sufficient to ensure protection from improper disclosure of controlled unclassified and classified information. DARPA also requested that instances of improper disclosure and disclosed information be provided to assess any potential damage. If no instances exist, DARPA requested the report acknowledge that no evidence of improper disclosure was found.

**Audit Response.** Although we acknowledge that DARPA has developed a training plan and that web-based reference materials are available, we do not agree that they can serve as a substitute for disseminating foreign disclosure instructions to program managers hosting foreign nationals. The information authorized for release to foreign nationals varies from country to country and project to project. Specific guidelines should be provided to the visit hosts to prevent the inadvertent release of technical information. We found no specific instances where technical information was improperly disclosed. However, at the time of our audit, the controls in place to ensure technical information was properly disclosed did not provide a reasonable assurance that the release of controlled unclassified information to foreign nationals was in accordance with visit authorization and delegation of disclosure authority letters.

## Recommendations and Management Comments

**A.1.** **We recommend that the Director, Defense Advanced Research Projects Agency, develop local procedures to ensure that foreign disclosure instructions from foreign visit approval authorities are disseminated to the program managers hosting foreign nationals.**

**DARPA Comments.** The Director, DARPA, concurred, stating that DARPA was in the process of updating its security manual, its international program's standard operating procedures, and its visitor control center standard operating procedures. In addition, DARPA was reminding its personnel to use available web-based reference materials as well as updating, improving, and increasing the frequency of security training.

**A.2.** **We recommend that the Director, Navy International Programs Office, revise Secretary of the Navy Instruction 5510.34, "Manual for the Disclosure of Department of the Navy Military Information to Foreign Governments and International Organizations," to include requirements for Government facilities being visited by foreign nationals to disseminate foreign disclosure restrictions contained in visit authorization letters to the proposed hosts of the visit.**

**Navy Comments.** The Office of the Assistant Secretary of the Navy (Research, Development and Acquisition), in coordination with the Director, Navy International Programs Office, concurred, stating that a proposal to revise Secretary of the Navy Instruction 5510.34 will be made. In addition, the Navy International Programs Office will take immediate action by including a statement in all future notification letters to Navy facilities requiring the dissemination of disclosure restrictions to hosts of foreign national visitors.

**A.3.  We recommend that the Commanding Officer, Naval Research Laboratory, develop local procedures to ensure that foreign disclosure instructions from foreign visit approval authorities are disseminated to the program managers hosting foreign nationals.**

**Navy Comments.**  The Office of the Assistant Secretary of the Navy (Research, Development and Acquisition), in coordination with the Commanding Officer, Naval Research Laboratory, concurred, stating the Navy Lab has initiated procedures to ensure the dissemination of foreign disclosure instructions from foreign visit approval authorities to visit hosts.

# B. Security Controls for Foreign National Visitors at the Defense Advanced Research Projects Agency

The Military Department laboratories' approval processes for visits by foreign nationals were adequate (see Appendix C). However, DARPA security controls over the approval process for foreign national visitors were weak. Specifically, DARPA controls for granting building access for foreign national visitors representing U.S. entities required improvement because DARPA did not enforce its policies and procedures governing advance notice. Also, the DARPA database contained inconsistent data because DARPA often changed policies on the fields used to input data into its database, and DARPA had inaccurate data in its database, because DARPA did not use the Defense Intelligence Agency visit approval letter as the source document. As a result, controls over the disclosure of controlled unclassified information to foreign nationals were not effective and DARPA may have inadvertently disclosed controlled unclassified information to other countries, including countries of concern,[7] without authorization.

## Policies and Procedures Governing Visits of Non-U.S. Citizens

**The NISPOM.** The NISPOM prescribes requirements, restrictions, and other safeguards that are necessary to prevent unauthorized disclosure of classified information and to control authorized disclosure of classified information to contractors. The NISPOM states that only U.S. citizens are eligible for a security clearance. However, in rare circumstances, non-U.S. citizens may be granted a Limited Access Authorization when the non-U.S. citizen possesses unique or unusual skills that are urgently needed to support a specific U.S. contract. Contractors are responsible for establishing procedures to ensure that foreign nationals are not afforded access to classified information and other export-controlled technical data except as authorized by an export license, approved visit request, or other exemption to export licensing requirements.

**DARPA Policies and Procedures Governing Visits of Non-U.S. Citizens.** DARPA policies and procedures governing visits of non-U.S. citizens are contained in the DARPA Security Manual; the Security and Information Directorate informal standard operating procedures for processing visits by foreign nationals; the DARPA Visitor Control Center procedures; "Guidelines for Non-U.S. Citizen Visitors," posted on a DARPA intranet webpage; and new employee orientation training provided by the Security and Intelligence Directorate.

---

[7]For this audit, countries of concern were taken from a list compiled by the Department of Energy for reasons of national security, nonproliferation, anti-terrorism, or economic security.

# DARPA Foreign Disclosure Controls

Security controls over the approval process for visits by foreign nationals representing U.S. entities and over the documentation of visits by foreign nationals representing foreign entities were weak. We reviewed records from the Security Information Management System database of 660 foreign nationals that had visited DARPA, of which 596 were foreign nationals representing U.S. entities and 64 were foreign nationals representing foreign entities.

**Approval Process for Visits by Foreign Nationals Representing U.S. Entities.** Of the 12 program managers interviewed who had held meetings with foreign nationals representing U.S. entities, 4 had not known they were hosting foreign nationals from countries of concern until the meeting occurred. DARPA had no approval process for visiting foreign nationals who represented U.S. entities. DARPA had foreign nationals from countries of concern showing up for visits to discuss sensitive information without visit requests or advance notice. To review the approval process for foreign nationals representing U.S. entities, we selected a judgmental sample of 12 foreign nationals from the 596 foreign nationals listed in the database as having visited DARPA in the past 15 months. We selected foreign nationals from countries of concern who had visited DARPA five or more times. For each of the 12 visitors, we interviewed the point of contact identified in the database to determine whether the visits took place, the dates of the visits, the information that was discussed, and what information had been released to the foreign nationals.

When a foreign national represents a U.S. entity and requires access to classified or export-controlled information, the NISPOM places the requirement for verification of the foreign national's citizenship and security clearance level on the contractor. Therefore, a visit request from the contractor employing the foreign national in advance of a visit would serve as documentation of the foreign national's citizenship and security clearance level. Most relationships between the research laboratories we reviewed and U.S. academic institutions are contractual relationships; therefore, the NISPOM would also apply when foreign nationals are representing U.S. academic institutions and visit requests from U.S. academic institutions would also serve as documentation of the foreign national's citizenship and security clearance level.

**Documentation of Visits by Foreign Nationals Representing Foreign Entities.** We reviewed the files kept by the Security and Intelligence Directorate for the 64 visits by foreign nationals representing foreign entities. We compared the citizenship and security clearance level of the visitor listed in the Defense Intelligence Agency visit approval letter with the citizenship and security clearance listed on the incoming Visitor Control Center record.

17

Table 3 shows the results of our review.

<div style="border:1px solid black; padding:10px;">

**Table 3.  Results of DARPA Review**

| Areas Reviewed | Yes | No[1] |
|---|---|---|
| Correct citizenship listed in files[2] | 57 | 7 |
| Correct security clearance level listed in files[2] | 45 | 19 |

[1]There were no files for 7 of the 64 visits, and those cases are included in the "no" column since accuracy could not be determined.
[2]As matched against the Defense Intelligence Agency visit approval letter.

</div>

For all official visitors for which DARPA had documentation, DARPA did list the correct citizenship.  However, DARPA listed incorrect security clearance levels for about 30 percent of the visits.  Because the Visitor Control Center files are sometimes consulted by program managers as a source of information for the status of upcoming meetings, the impact of those inaccurate records could result in information at a higher level than authorized being disclosed to a foreign national.

## DARPA Compliance With Policies and Procedures

DARPA did not comply with its policies and procedures governing visit requests by non-DARPA personnel wishing to visit DARPA.  The Visitor Control Center did not consistently enforce security policies requiring advance notice for visits of non-DARPA personnel.  The DARPA Security Manual states that non-DARPA individuals must have their security clearances and visit requests sent to the DARPA Visitor Control Center at least 2 weeks in advance of an intended visit.  However, the Security and Intelligence Director stated that advance notice requirements were enforced only for meetings that were expected to be classified.  The Security and Intelligence Director stated that many unclassified meetings took place every day at DARPA where visit requests were not required.

## DARPA Documentation of Foreign Visits

Existing policies and procedures provided inadequate controls over the documentation and recording of foreign visitors representing foreign entities because record keeping was inconsistent and often inaccurate.  The DARPA record of visits by foreign nationals was contained in the Security Information Management System database.

**DARPA Record Keeping Concerning Foreign Nationals.**  DARPA documentation of foreign national visitors representing foreign entities was inconsistent when recording whether a foreign national was representing a U.S. entity or a foreign entity.  From the 660 records reviewed, we identified

46 visitors as representing foreign entities when the "purpose" field of the DARPA Visitor Control Center record stated that the individual represented a foreign government. We identified an additional 11 visitors as representing foreign entities when one of several other fields, usually the "facility" field, listed a recognizable foreign government agency. We also reviewed visits by foreign nationals with a security clearance higher than unclassified who appeared to be representing U.S. entities and found another seven visits by foreign nationals representing foreign entities. According to the Visitor Control Center manager, the inconsistent record keeping was due to changing policies on how to record foreign nationals in the Security Information Management System database. There was no written guidance available describing the correct content of each field in the database. Additional visits by foreign nationals representing foreign entities may have occurred, but those visits could not be identified with DARPA records because there was not a consistent method used to identify foreign nationals who represented foreign entities.

**DARPA Record Keeping Concerning Security Clearances.** DARPA input to the Security Information Management System database was often inaccurate. Table 3 shows that DARPA inputted the incorrect security clearance level or did not have records of the individual's security clearance level for 19 of 64 visits by foreign nationals representing foreign entities. Because the Security Information Management System database is sometimes used by DARPA program managers as a source of information for scheduled meetings, those errors could be significant. If the database incorrectly lists a foreign national as holding a higher security clearance level than he does, a program manager could ascertain from the database that he could release information to the foreign national for which the foreign national is not authorized. That risk was further increased because DARPA did not disseminate foreign disclosure instructions to program managers for a majority of meetings, as discussed in finding A.

## Effect of Foreign Disclosure Control Weaknesses at DARPA

The information on developing technology available at DARPA is highly sensitive. Controls over the disclosure of controlled unclassified information to foreign nationals at DARPA were not effective. Because DARPA did not require advance notice for meetings that were expected to be unclassified, foreign nationals unexpectedly attended several meetings. When we interviewed program managers who had hosted foreign nationals representing U.S. entities, 4 of 12 program managers interviewed stated they were unaware until the meetings took place that they were hosting foreign nationals at the meetings in question. The four foreign nationals were from three countries of concern: China, Israel, and Syria.

- In January 2000, a DARPA Advanced Technology Office representative met with a group of three people he thought were representing the Navy Lab to discuss building thin film resonators. The DARPA representative questioned one member of the group who had on a foreign national badge, and found out he was a Chinese citizen representing GeoCenter, a contractor that supports the Navy Lab. The DARPA representative stated that once he found out one of the group was a foreign national, he did not provide them with any

information. The Advanced Technology Office representative emphasized that his office dealt with very sensitive information and they are very sensitive about the release of information. However, he stated this meeting was unclassified and no sensitive information had been discussed.

- In July 1999, a DARPA Information Systems Office representative met with three representatives from Instinct Software, an Israeli company that had recently opened an American affiliate, to discuss products their company had produced for Israeli intelligence. The DARPA representative did not know one of the group was an Israeli citizen until the meeting took place. Although DARPA had invited Instinct Software to the meeting, the foreign national was representing a foreign company and DARPA should not have met with the individual without a visit approval letter from the Defense Intelligence Agency. The Information Systems Office representative stated that the meeting was unclassified and no sensitive information had been discussed.

- In July 1999, the DARPA Information Technology Office deputy director met with faculty members of U.S. universities to discuss a proposal concerning robotics. A professor from Pennsylvania State University had requested the meeting. The deputy director did not know that one of the group was a Syrian citizen representing Tennessee State University. The deputy director stated that the meeting was unclassified and no sensitive information had been discussed.

- In June 1999, the DARPA Information Resources director met with a group of people representing the V-One Company, a company presumed by DARPA to be a U.S. company, to discuss a potential contract. When the Information Resources director met with the group, he recognized that one of them was not a U.S. citizen because of the type of badge he wore. However, until our review, the Information Resources director did not know that the individual was a Chinese citizen. The Information Resources director stated that the meeting was unclassified and no sensitive information had been discussed.

Because DARPA had inaccurate records, foreign nationals showed on DARPA records as having different security clearance levels than listed on Defense Intelligence Agency records. In one case, the Israeli Assistant Attaché visited DARPA on three occasions during 1997 and 1998. Although Defense Intelligence Agency records state the Attaché had a Secret security clearance, DARPA records state he had a Top Secret security clearance.

Although most of the visits reviewed were unclassified, DARPA is a repository of information on developing technology, an area the Defense Security Service has stated is targeted by other countries for data collection. DARPA foreign disclosure control weaknesses included program managers unknowingly hosting foreign nationals and DARPA documentation of foreign visits being inconsistent and inaccurate. Because foreign nationals can claim to represent a U.S. entity

and visit DARPA with almost no controls, foreign nationals may be gathering sensitive information without DARPA knowledge. The inconsistent and inaccurate documentation of visits and visitors could result in program managers believing that individuals had access to higher classifications of information than the individuals had actually been cleared for, thereby causing program managers to inadvertently release unauthorized data to foreign nationals.

## Recommendations and Management Comments

**B. We recommend that the Director, Defense Advanced Research Projects Agency:**

**1. Enforce and improve security procedures to ensure visits by foreign nationals representing U.S. entities are sufficiently documented to verify the citizenship and security clearance level of the foreign nationals.**

**2. Prepare a Defense Advanced Research Projects Agency manual providing specific procedures for preparation of Visitor Control Center records with an explanation of each field to be completed to aid consistent record keeping.**

**3. Develop Security Information Management System database input methods that ensure the Defense Intelligence Agency visit approval letter is used as the primary source document for all information regarding official foreign national visitors.**

**DARPA Comments.** The Director, DARPA, concurred with the recommendations, stating that DARPA was actively taking corrective actions in three areas: continuing to improve training for office directors, deputy directors, assistant directors for program management, program managers, and Visitor Control Center personnel; completing the DARPA Security Manual and the associated standard operating procedures and instructions; and reviewing the Security Information Management System database requirements.

# Appendix A. Audit Process

## Scope

This is one in a series of reports being issued by the Inspector General, DoD, in accordance with the National Defense Authorization Act for Fiscal Year 2000, section 1402, which requires an annual report on the transfer of militarily sensitive technology to countries and entities of concern.

We evaluated procedures for identifying and processing documentation of visits by foreign nationals, determining the level of visiting foreign nationals' authorized access to installations and to information, and procedures for notifying hosts of the visitors the extent of the visitors' authorized access to information.

We conducted interviews with personnel at the Army Materiel Command; the Army Deputy Chief of Staff (Intelligence) Foreign Disclosure Directorate; the Navy International Programs Office; and the Secretary of the Air Force, International Affairs Division. In addition, we visited DARPA in Arlington, Virginia; the Army Lab in Adelphi, Maryland; the Navy Lab in Washington, D.C.; and the Air Armament Center and the Air Force Munitions Lab at Eglin Air Force Base, Florida. At those sites, we conducted interviews with DoD managers responsible for foreign disclosure and security. We also interviewed personnel with whom the foreign national visitors met.

**DoD-Wide Corporate Level Government Performance and Results Act Coverage.** In response to the Government Performance and Results Act, the Secretary of Defense annually establishes DoD-wide corporate level goals, subordinate performance goals, and performance measures. This report pertains to achievement of the following goal and subordinate performance goal:

> **FY 2000 Corporate Level Goal 2:** Prepare now for an uncertain future by pursuing a focused modernization effort that maintains U.S. qualitative superiority in key warfighting capabilities. Transform the force by exploiting the revolution in Military Affairs, and reengineer the Department to achieve the 21st century infrastructure. **(00-DoD-2)**
> **FY 2000 Subordinate Performance Goal 2.2:** Transform the U.S. military forces for the future. **(00-DoD-2.2)**

## Methodology

**Audit Approach.** For each site visited, we:

- interviewed foreign disclosure and security officials;

- reviewed policies and procedures for processing foreign visitors;

- identified official and unofficial foreign visitors;

- selected a judgmental sample of official and unofficial foreign visitors based on countries of concern and targeted technologies;

- obtained and reviewed documentation for each visitor selected; and

- interviewed the host points of contact to determine if they had been made aware of the disclosure guidelines.

**Use of Computer-Processed Data.** To achieve the audit objectives, we relied on computer-processed data contained in the DARPA Security Information Management System database and the databases used for the management of foreign national visitors at the Army Lab, the Navy Lab, and the Air Force Munitions Lab. Although we did not perform a formal reliability assessment of the computer-processed data, we did find some accuracy errors in the DARPA database. We did not find errors that would preclude the use of the computer-processed data to meet the objectives of the audit or that would change the conclusions in the report.

**Audit Types, Dates, and Standard.** We performed this program audit from February through June 2000 in accordance with auditing standards issued by the Comptroller General of the United States, as implemented by the Inspector General, DoD. Accordingly we included tests of management controls considered necessary.

**Contacts During the Audit.** We visited or contacted individuals and organizations within DoD. Further details are available upon request.

# Management Control Program

DoD Directive 5010.38, "Management Control (MC) Program," August 26, 1996, requires DoD organizations to implement a comprehensive system of management controls that provides reasonable assurance that programs are operating as intended and to evaluate the adequacy of those controls.

**Scope of Review of the Management Control Program.** We reviewed the adequacy of management controls over foreign disclosure instructions contained in visit authorization letters and delegation of disclosure authority letters as well as foreign national access restraints at each of the sites visited. We also reviewed the DARPA and Military research laboratories' Annual Statements of Assurance for FY 1998 and FY 1999.

**Adequacy of Management Controls.** The procedural deficiencies indicated by the audit are management control weaknesses, but we did not regard them as material, as materiality is defined in DoD Instruction 5010.40, "Management Control (MC) Program Procedures," August 28, 1996. Nevertheless, they need to be addressed. The recommendations made in this report will, if implemented, eliminate the procedural deficiencies.

# Appendix B. Prior Coverage

During the last 5 years the General Accounting Office and the Inspector General, DoD, have conducted multiple reviews related to the adequacy of management controls over transfers of sensitive and critical DoD technology with potential military application to foreign nationals. Unrestricted General Accounting Office reports can be accessed over the Internet at http://www.gao.gov. Unrestricted Inspector General, DoD, reports can be accessed over the Internet at http://www.dodig.osd.mil/audit/reports. The following previous reports are of particular relevance to the subject matter in this report.

## General Accounting Office

General Accounting Office Report No. NSIAD-98-196 (OSD Case No. 1648), "Export Controls: Information on the Decision to Revise High Performance Computer Controls," September 1998.

General Accounting Office Report No. NSIAD-95-82 (OSD Case No. 9798), "Export Controls: Some Controls Over Missile-Related Technology Exports to China Are Weak," April 1995.

## Inspector General

Inspector General, DoD, Report No. D-2000-130, "Foreign National Access to Automated Information Systems," May 26, 2000.

Inspector General, DoD, Report No. D-2000-110, "Export Licensing at DoD Research Facilities," March 24, 2000.

Inspector General, DoD, Report No. 98-214, "Implementation of the DoD Technology Transfer Program," September 28, 1998.

Inspector General, DoD, Report No. 98-157, "Updating the Foreign Disclosure and Technical Information System," June 17, 1998.

Inspector General, DoD, Report No. 97-210, "Technology Transfer Under the F-15I Program," August 27, 1997.

## Interagency Reviews

Inspectors General of the Departments of Commerce, Defense, Energy and State, Report No. D-2000-109, "Interagency Review of the Export Licensing Process for Foreign National Visitors," March 24, 2000.

## Interagency Reviews (cont'd)

Inspectors General of the Departments of Commerce, Defense, Energy, State, and the Treasury and the Central Intelligence Agency, Report No. 99-187, "Interagency Review of the Export Licensing Processes for Dual-Use Commodities and Munitions," June 18, 1999.

## Army

Army Audit Agency Report No. AA 00-33, "Technology Transfers for Classified and Sensitive Information," December 20, 1999.

# Appendix C. Security Controls for Foreign National Visitors at the Military Department Laboratories

The Military Department laboratories' approval processes for visits by foreign nationals were adequate. A review of the Army Lab, the Navy Lab, and Air Force Munitions Lab foreign visits that occurred from October 1998 through December 1999 disclosed the following.

- The Military Department laboratories were aware of the citizenship of foreign national visitors prior to visits.

- The Military Department laboratories were aware of and correctly documented the security clearance levels of foreign national visitors.

A discussion of the applicable Military Departments' foreign visit policies and procedures is in Appendix D.

## Foreign Disclosure at the Army Lab

The Intelligence and Security Office database had records of 315 visits by foreign nationals from October 1, 1998, through December 31, 1999. Of the 315 visits, 186 visits were official and 129 visits were considered unofficial. We reviewed the case files for both the official and unofficial visits. We judgmentally selected 20 foreign national visitors. Those 20 foreign nationals held citizenships of 12 different countries, 8 of which are considered countries of concern. Of the 20 visitors, 9 had been on official visits and 11 had been on unofficial visits. Of the nine official visits, four were either one-time or recurring; five were extended visits. Of the 11 unofficial visits, 7 were either one-time or recurring; 4 were extended visits. All of the technology discussed during the visits was either basic or applied research.[*]

We reviewed files kept by the Foreign Disclosure Office for the 20 foreign national visitors. We verified the following information.

- The citizenship of the visitor listed in the Foreign Disclosure Technical Information System and local Army Lab database matched the information provided the visit point of contact on the Army Lab Form 118R-E, "U.S. Army Research Laboratory Foreign Visitors Clearance."

---

[*]Basic research includes all effort of scientific study directed toward increasing fundamental knowledge and understanding. Applied research is defined as a systematic study to gain knowledge or understanding necessary to determine the means by which a recognized and specific need may be met.

- The security clearance level of the visitor listed in the Foreign Disclosure Technical Information System and local Army Lab database matched the information provided the visit point of contact on the Army Lab Form 118R-E, "U.S. Army Research Laboratory Foreign Visitors Clearance."

Table C-1 shows the results of our review of the citizenship and security clearance level for all visitors reviewed.

| Table C-1. Results of Army Lab Review | | |
|---|---|---|
| Areas Reviewed | Yes | No |
| Correct citizenship listed in case files | 20 | 0 |
| Correct security clearance level listed in case files | 20 | 0 |

The Army Lab had controls that ensured all visits by foreign nationals were approved before the visits took place. The Army Lab listed the correct citizenship and security clearance level for all visitors we reviewed.

## Foreign Disclosure at the Navy Lab

The Foreign Visits database had records of 952 visits by foreign nationals from October 1, 1998, through December 31, 1999. Of the 952 visits, 739 were visits by foreign nationals representing U.S. entities, either contractors or academic institutions. The other 213 visits were by foreign nationals representing foreign entities. We selected a judgmental sample of 17 visits by foreign nationals representing U.S. entities from the Foreign Visits database. We selected visits by foreign nationals from countries of concern and visits by foreign nationals to discuss targeted technologies as identified by the Defense Security Service.

We reviewed the files kept by the Navy Lab Security group for the 213 visits by foreign nationals representing foreign governments. We verified the following information.

- The citizenship of the individual listed in the Navy International Programs Office approval letter matched the citizenship listed in the Foreign Visits database.

- The security level for the meeting listed in the Navy International Programs Office approval letter matched the security level listed in the Foreign Visits database.

Table C-2 lists the results of our review.

| Table C-2. Results of Navy Lab Review | | |
|---|---|---|
| Areas Reviewed | Yes | No |
| Correct citizenship listed in the database | 212 | 1 |
| Correct security clearance level listed in the database | 199 | 14 |

The Navy Lab had controls that ensured the majority of visits by foreign nationals were approved before the visit took place. The Navy Lab listed the correct citizenship for all but one foreign visitor. The Navy Lab listed a correct security level for about 93 percent of the meetings. Although 7 percent of the security clearances were incorrectly listed, we did not consider that to be material.

## Foreign Disclosure at the Air Force Munitions Lab

We reviewed the DoD Foreign Disclosure and Technical Information System records of the 410 foreign visitors representing foreign entities. We selected 18 visits from the DoD Foreign Disclosure and Technical Information System records based on Defense Security Service-identified targeted technologies and the approved security level of the meetings. Of the 18 visits, 4 did not take place. The 18 visits represented 129 approved visitors; however, 74 foreign national visitors actually came to the Air Force Munitions Lab.

Through interviews with the points of contact hosting the foreign nationals, we verified that:

- the citizenship of the individual who visited matched the citizenship listed in the Foreign Disclosure and Technical Information System, and

- the security level of the meeting matched the security level listed in the Foreign Disclosure and Technical Information System.

Table C-3 shows the results of our review.

| Table C-3. Results of Air Force Munitions Lab Review | | |
|---|---|---|
| Areas Reviewed | Yes | No |
| Correct citizenship | 74 | 0 |
| Correct security clearance level | 14 | 0 |

The Air Force Munitions Lab had controls that ensured all visits by foreign nationals representing foreign entities were approved before the visit took place. The Air Force Munitions Lab listed the correct security clearance and citizenship for all visitors we reviewed.

# Appendix D. Military Departments' Foreign Visits Policies and Procedures

Each of the Military Departments develops its own regulations and instructions in order to implement NDP-1, DoDD 5230.20, and the NISPOM. The individual organizations develop standard operating procedures to implement their respective Department's regulations and instructions. This appendix describes the regulations, instructions, handbooks, and standard operating procedures that implement guidelines concerning the release of information to foreign national visitors.

## Army Policies and Procedures

**Army Regulation 380-10, "Technology Transfer, Disclosure of Information and Contacts with Foreign Representatives," December 30, 1994.** Army policy on the disclosure of Army technical information is described in Army Regulation 380-10. The regulation provides policy on disclosure criteria, conditions, and limitations for release of Army technical information to foreign nationals. Chapter 5, "Contact with Foreign Representatives," requires the host organization foreign disclosure officer and contact officer to prepare a delegation of disclosure authority letter for each foreign national assigned as a liaison officer, an exchange officer, or a Scientific and Engineer Exchange Program researcher.

**Army Lab Director's Memorandum, "Visits to Army Research Laboratory by Non-U.S. Citizens in Support of Unclassified Contractual Arrangements, Seminar Presentations, Commercial Sales/Marketing, Academic Collaborative Arrangements," April 12, 2000.** The memorandum was a result of the director's review of the Army Lab controls over foreign national visitors. The memorandum describes the policy for granting authorization for visits to the Army Lab by non-U.S. citizens. It provides the policy and procedures to control the transfer of technical information to non-U.S. citizens during unofficial visits. Unofficial visits are those visits authorized under local delegated authority and conducted by non-U.S. citizens who are not representing foreign entities. All unofficial visits must be held at the unclassified, public domain level. The memorandum states that it is the responsibility of the visit points of contact to ensure the visitors do not have access to controlled unclassified and classified information while at the Army Lab. It also states that the director must approve all recurring and extended visits.

**Chief, Intelligence and Security Branch, Memorandum, "Quarterly Reporting of Non-Citizen Visitors to Army Research Laboratory," June 30, 2000.** The memorandum was in response to an Army Materiel Command requirement to provide quarterly reports on foreign visits to the Army Lab. The Army Lab director requested that daily records of all foreign national visitors be provided to the Army Lab foreign disclosure officer.

**Army Research Laboratory Pamphlet 380-41, "Foreign Disclosure Handbook," April 1, 1997.** The handbook contains a broad outline of policies governing foreign disclosure, as well as standard procedures for releasing U.S. Army information and materials to foreign governments and international organizations. The handbook discusses various disclosure topics included in the following chapters: Activities with Industry; Delegation of Disclosure Authority Letters; Disclosure of Documents and Materials; International Cooperative Research and Development; National Disclosure Policy; Personnel Exchange Programs; Scientific and Technical Meetings; and Visits. The handbook provides instructions for the development of data exchange agreements and international exchange agreement delegation of disclosure authority letters; for the development of project agreement delegation of disclosure authority letters; and for the completion of the various Army Lab forms. The handbook also provides the foreign disclosure officer with procedures for processing official visits. Official visits are those visits sponsored by foreign governments or foreign contractors.

**Army Lab Director's Memorandum, "Activities Involving Non-U.S. Citizens," February 10, 1999.** In February 1999, the director placed a moratorium on all unofficial visits by non-U.S. citizens. The moratorium was in effect until he reviewed the Army Lab policy concerning visits by foreign nationals. The review was necessary to ensure the visit by a foreign national was in the best interest of the Army Lab and the U.S. Army. The moratorium resulted in a complete review of the Army Lab controls over foreign visitors.

**Army Lab Standard Operating Procedures for Visits by Foreign Nationals.** The Army Lab had standard operating procedures for processing visits by foreign nationals. Separate procedures existed for official visits and unofficial visits. All procedures listed are in accordance with DoD and Secretary of the Army regulations.

**Army Lab Official Visit Standard Operating Procedures.** The foreign embassy must submit a Request for Visit Authorization to Army headquarters through the Foreign Visit System of the Foreign Disclosure Technical Information System. The Army Lab foreign disclosure officer provides the Army Lab position to Army headquarters; however, Army headquarters has the final approval. The Army Lab alternate foreign disclosure officer prints out the Foreign Visit System inbox every morning. He enters the information into the Army Lab database. The alternate foreign disclosure officer then staffs Army Lab Form 147, "Foreign Visit Request," with the possible visit point of contact. Upon completion of Army Lab Form 147 by the visit point of contact, the foreign disclosure officer or the alternate foreign disclosure officer inputs the approval or denial into the Foreign Visit System, with the recommended disclosure level if the visit has been approved. The Army Lab then awaits the final decision by Army headquarters. Once the Army approves the visit request, Army Lab Form 118-R-E, "U.S. Army Research Laboratory Foreign Visitor's Clearance," is filled out and signed by both the visit point of contact and the foreign disclosure officer or the alternate foreign disclosure officer. The foreign disclosure officer or the alternate foreign disclosure officer then updates the local database, changing the status field from "staffed" to "approved." A copy of the signed Army Lab Form 118-R-E is provided to the visit point of contact and visitor reception desk.

**Army Lab Unofficial Visit Standard Operating Procedures.** There are separate policies and procedures for unofficial one-time, recurring, and extended visits. Those policies and procedures are explained in the Army Lab director's memorandum of April 12, 2000. Although the procedures for the different types of unofficial visits are similar (authority, badges, computer access, escort requirements, and information access), there are differences in the information required for each type of visit and the time frame in which the information must be submitted. However, for each visitor, a completed Army Lab Form 183-R-E, "Non-U.S. Citizen Information Sheet" must be submitted. The procedures followed upon submission of the request are the same for all three types of visits.

**One-Time Visits.** The foreign disclosure officer and alternate foreign disclosure officer have been delegated the authority to approve one-time visits by non-U.S. citizens. The visitor's access is limited to unclassified, public domain information. Computer access is not authorized. The visitor is issued an "Escort Required" badge and is escorted at all times. Two weeks prior to the visit, the visit point of contact must submit written justification of the visit to the foreign disclosure officer. The justification should include the purpose of the visit; whether the visitor will conduct or demonstrate research; whether a tour of the Army Lab will be conducted; verification that all disclosures will be limited to unclassified, public domain information; and Army Lab Form 183-R-E.

**Recurring Visits.** The Army Lab director approves all recurring visit requests by non-U.S. citizens. The visitor's access is limited to unclassified, public domain information. Computer access is determined on a case-by-case basis. The visitor is issued an "Escort Required" badge and is escorted at all times. Thirty days prior to the first visit, the visit point of contact must submit in a package to the foreign disclosure officer or alternate foreign disclosure officer, a request memorandum signed by the director of the point of contact's directorate. The request should identify the contractual arrangement requiring the recurring visits; describe the purpose of the visit and why multiple visits are necessary; indicate whether the visitor will conduct or demonstrate research or attend a conference; and outline requirements for computer access. Attachments to the request should include a completed Army Lab Form 183-R-E and contractor or university verification of the visitor's work authorization.

**Extended Visits.** The Army Lab director approves all extended visit requests by non-U.S. citizens. The visitor's access is limited to unclassified, public domain information. Computer access is limited to a stand-alone computer with an individual Internet Service Provider for e-mail Internet access. The visitor is issued a white, non-citizen picture badge that allows him or her to travel without an escort along a restricted route (from the gate to the cafeteria, specific bathrooms, and work location). The visitor must be escorted to those locations not included in his route (library and other buildings or offices). Sixty days prior to the first day of the visit, the visit point of contact must submit in a package to the foreign disclosure officer or alternate foreign disclosure officer, a request memorandum signed by the director of the point of contact's directorate. The request should identify the equipment to be

used by the visitor; the expected benefit to the Army Lab; the guest researcher's expertise or unique skill; and any intended contractual arrangement. It should include a justification for continued access to the Army Lab facility; a position description; and where the work will be performed. The attachments to the request should include verification of the visitor's work authorization and completed Army Lab Forms 134, 135, and 183-R-E. Security standard operating procedures are written for all foreign nationals on extended visits and given to the visit host. The security standard operating procedures describe the various security procedures applicable to the individual visitor and clearly identify what is and is not permissible.

Once the information is submitted, for any of the three types of visits, the foreign disclosure officer or the alternate foreign disclosure officer coordinates the request with representatives from the Army Lab legal counsel office, the International Programs Office, and the Security and Intelligence Branch. A coordinated recommendation is then made to the Army Lab director for approval. The foreign disclosure officer or the alternate foreign disclosure officer then provides the visit point of contact with a completed Army Lab Form 118-R-E with specific disclosure instructions. The visit point of contact reviews the responsibilities, signs the certification box, and returns the form to the foreign disclosure officer or the alternate foreign disclosure officer. A copy of the signed Army Lab Form 118-R-E is provided to the visitor reception desk.

## Navy Policies and Procedures

Secretary of the Navy Instruction 5510.34, Part II, Chapter 5, "International Agreements," requires the Navy International Programs Office to provide the technical project officers for memorandums of understanding, information exchange projects, and mutual weapons development data exchange agreements with a delegation of disclosure authority letter.

**Naval Research Memorandum, "Visits to NRL [Naval Research Laboratory] by Foreign Nationals," July 27, 1999.** The memorandum provides local procedures for controlling foreign national visits to the Navy Lab. The memorandum contains specific instructions for justifying classified meetings with foreign nationals and specifies the necessary internal approvals for visits by foreign nationals. Also included are local badging requirements for foreign national visitors. All procedures listed are in accordance with DoD and Secretary of the Navy regulations. However, the memorandum does not require the Navy Lab Security Office to provide foreign disclosure authorizations to program managers hosting foreign national visitors.

**Navy Lab Standard Operating Procedures for Visits by Foreign Nationals.**
The Navy Lab had standard operating procedures for processing visits by
foreign nationals. Separate procedures existed for official visits and unofficial
visits.

**Navy Lab Official Visit Standard Operating Procedures.** Official
visits are those which involve substantive or technical discussions or the
disclosure of classified information, and must be approved by an authority
outside of the Navy Lab, usually the Navy International Programs Office.
Requests for both short- and long-term visits to the Navy Lab by foreign
nationals originate from the visitor's embassy. Visits by representatives of
foreign governments must be arranged and approved through the Navy
International Programs Office. Navy Lab security personnel coordinate the
requests with the appropriate Navy Lab points of contact who recommend
approval of the visits. The authority to recommend approval or disapproval of a
visit usually is delegated to the individual or individuals named on a visit
request. In some instances, approval must also be obtained from division heads,
associate directors of research, or the commanding officer.

Classified information may not be disclosed to visitors from a
Communist-controlled country. Navy Lab personnel desiring to sponsor visits
that involve disclosure of U.S. classified information to a foreign national must
submit a memorandum to the Navy Lab Security Office at least 3 months in
advance of the date of the proposed visit.

**Navy Lab Unofficial Visit Standard Operating Procedures.**
Unofficial visits are those that are made for courtesy or general purposes, do not
involve technical or substantive discussions or disclosure of classified
information, and are short in duration. They are approved by the Navy Lab
commanding officer. Requests for any foreign national to visit the Navy Lab or
Navy Lab field sites (official and unofficial), whether initiated by Navy Lab
personnel, by another organization, or by a foreign government, must be
submitted to the Navy Lab Security Office for approval. Navy Lab division
heads must submit requests 1 week prior to the visit to allow time for
processing.

**Short-Term Visit Requests.** Requests for short-term visits (30 days
or less) are submitted on Navy Lab Form 5521/1206, "Unclassified Visits by
Foreign Nationals." Visits are approved by the Division Superintendent and
reviewed by the Security Office. The form should reach the Security Office at
least a week in advance and may be referred to the director of research or the
commanding officer of the Navy Lab. Short-term visitors must be escorted,
unless the director of research or the commanding officer has approved an
exception.

**Long-Term Visit Requests.** Requests for long-term visits (over
30 days) are submitted on Navy Lab Form 5527/2. The request is routed via
division heads and the assistant director of research to the director of research
for the Navy Lab. The form must be submitted in time to receive approval by
the director of research before the start of the visit. After approval, the visitor's
name and information is submitted to the Naval Criminal Investigative Service

for a background check. The background check takes 1 to 6 months. The visitor must be escorted pending the results of the background check. If the results of the background check are favorable, the Security Office may permit the visitor to be unescorted during normal working hours.

## Air Force Policies and Procedures

**Air Force Handbook 16-202, "Disclosure Handbook," October 20, 1993.** The handbook provides procedures for managing the Air Force Disclosure Program. It applies to foreign disclosure officers and to technical personnel who receive, review, process, coordinate, and approve or deny requests for release of military information to foreign governments and their representatives. The handbook states that for base-level foreign disclosure programs, base foreign disclosure officers have the responsibility of implementing and administering disclosure functions. Disclosure authority is derived primarily from delegation of disclosure authority letters. The handbook states a delegation of disclosure authority letter is required for foreign government representatives assigned to Air Force organizations under extended visit authorizations, or attached as students or exchange officers.

**Air Force Instruction 16-201/Air Armament Center Supplement 1, "Disclosure of Military Information to Foreign Governments and International Organizations," July 12, 1999.** The instruction supplement lists the internal offices with authority for approving visits by foreign nationals and the internal offices with foreign disclosure authority. It also includes local badging requirements for foreign national visitors. The instruction supplement states that foreign nationals will be issued a foreign visitor badge from the foreign disclosure office. The visit point of contact is responsible for ensuring foreign nationals wear their badges and are escorted while at the Air Force Munitions Lab. All procedures listed are in accordance with DoD and Secretary of the Air Force regulations.

**Air Force Munitions Lab Standard Operating Procedures for Visits by Foreign Nationals.** The Air Force Munitions Lab had standard operating procedures for processing official visits by foreign nationals.

**Air Force Munitions Lab Official Visit Standard Operating Procedures.** Official visit requests for foreign nationals originate from the visitor's embassy and go to the Office of the Secretary of the Air Force, International Affairs Division. Requests to visit Air Force facilities or installations are staffed through the major commands, if applicable, for technical review. Requests to visit the Air Force Munitions Lab are staffed through the Air Force Materiel Command. The Air Force Munitions Lab foreign disclosure officer contacts the visit point of contact to determine if he or she is willing to support the visit. The visit point of contact then completes a Proposed Foreign Visit Worksheet, stating approval or disapproval, and returns the worksheet to the foreign disclosure officer. The visit point of contact must also identify the disclosure level for classified visits. The foreign disclosure officer then enters the approval or disapproval into the DoD Foreign Disclosure and Technical Information System. If the visit is approved, the foreign disclosure officer

35

provides the point of contact with an Approved Visit Request memorandum that describes the guidelines for the visit. The point of contact is also given a copy of the Foreign Disclosure and Technical Information System paperwork. The point of contact acknowledges his or her responsibilities and the visit guidelines by signing the memorandum endorsement and returning it to the foreign disclosure officer.

**Air Force Munitions Lab Unofficial Visit Standard Operating Procedures.** We did not identify any standard operating procedures for unofficial visits. Air Force Munitions Lab personnel stated all visits were considered official and required visit requests submitted by the visitors' embassies.

# Appendix E.  Report Distribution

## Office of the Secretary of Defense

Under Secretary of Defense for Acquisition, Technology, and Logistics
    Director, Defense Research and Engineering
        Director, Defense Advanced Research Projects Agency
        Defense Advanced Research Projects Agency Comptroller
Under Secretary of Defense for Policy
    Assistant Secretary of Defense (International Security Affairs)
    Deputy Under Secretary of Defense (Policy Support)
Under Secretary of Defense (Comptroller/Chief Financial Officer)
    Deputy Chief Financial Officer
    Deputy Comptroller (Program/Budget)

## Department of the Army

Deputy Under Secretary of the Army (International Affairs)
Assistant Secretary of the Army (Financial Management and Comptroller)
Director, Department of the Army, Military Intelligence-Foreign Disclosure
Commanding General, Army Materiel Command
    Director, Army Research Laboratory
Auditor General, Department of the Army

## Department of the Navy

Assistant Secretary of the Navy (Manpower and Reserve Affairs)
Director, Navy International Programs Office
Naval Inspector General
Office of Naval Research
    Commanding Officer, Naval Research Laboratory
Auditor General, Department of the Navy

## Department of the Air Force

Assistant Secretary of the Air Force (Financial Management and Comptroller)
Deputy Under Secretary of the Air Force (International Affairs)
Commander, Air Force Materiel Command
Commander, Air Force Research Laboratory
    Director, Air Force Research Laboratory-Munitions
Auditor General, Department of the Air Force

# Non-Defense Federal Organization

Office of Management and Budget

# Congressional Committees and Subcommittees, Chairman and Ranking Minority Member

Senate Committee on Appropriations
Senate Subcommittee on Defense, Committee on Appropriations
Senate Committee on Armed Services
Senate Committee on Banking
Senate Committee on Governmental Affairs
Senate Select Committee on Intelligence
House Committee on Appropriations
House Subcommittee on Defense, Committee on Appropriations
House Committee on Armed Services
House Committee on Government Reform
House Subcommittee on Government Management, Information, and Technology, Committee on Government Reform
House Subcommittee on National Security, Veterans Affairs, and International Relations, Committee on Government Reform
House Committee on International Relations
House Subcommittee on International Economic Policy and Trade, Committee on International Relations
House Permanent Select Committee on Intelligence

# Department of the Navy Comments

**DEPARTMENT OF THE NAVY**
OFFICE OF THE ASSISTANT SECRETARY
RESEARCH, DEVELOPMENT AND ACQUISITION
1000 NAVY PENTAGON
WASHINGTON DC 20350-1000

OCT - 4 2000
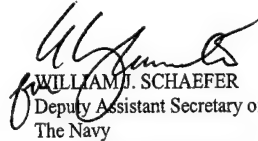
MEMORANDUM FOR THE DEPARTMENT OF DEFENSE ASSISTANT
INSPECTOR GENERAL FOR AUDITING

Subj: DRAFT AUDIT REPORT ON FOREIGN NATIONAL SECURITY
CONTROLS AT DOD RESEARCH LABORATORIES (PROJECT NO
D1999LG-0034.03)

Ref: (a) DODIG memo of 24 Jul 00

Encl: (1) Department of the Navy Response

In response to reference (a), the Navy comments are provided in enclosure (1). We
concur with the recommendations.

WILLIAM J. SCHAEFER
Deputy Assistant Secretary of
The Navy
Planning, Programming and
Resources

Copy to:
NAVINSGEN(42)
NIPO
NRL

DEPARTMENT OF THE NAVY RESPONSE TO
RECOMMENDATIONS FOR
DODIG DRAFT AUDIT REPORT OF 24 JUL 00
"FOREIGN NATIONAL SECURITY CONTROLS AT
DOD RESEARCH LABORATORIES"
(PROJECT D1999LG-0034.03)

Recommendation:

A.2. We recommend that the Director, Navy International Programs Office, revise Secretary of the Navy Instruction 5510.34, "Manual for the Disclosure of Department of the Navy Military Information to Foreign Governments and International Organizations," to include requirements for Government facilities being visited by foreign nationals to disseminate foreign disclosure restrictions contained in visit authorization letters to the proposed hosts of the visit.

Department of the Navy Response:

The Navy concurs with this recommendation and will propose a revision to SECNAVINST 5510.34. Additionally, effective immediately, the Navy International Programs Office will include the following statement in all visits for which it generates notification letters to DON facilities: "The receipt of this visit approval notification letter is required to disseminate the disclosure restrictions contained herein to the host(s) of the visit."

Recommendation:

A.3. We recommend that the Commanding Officer, Naval Research Laboratory, develop local procedures to ensure that the foreign disclosure instructions from foreign visit approval authorities are disseminated to the program managers hosting foreign nationals.

Department of the Navy Response:

The Navy concurs with the recommendation and has initiated procedures to ensure dissemination of foreign disclosure instructions from foreign visit approval authorities. A copy of the Naval Research Laboratory memorandum directing appropriate action by the Personnel Security and Visitor Control Section is included in our response.

United States Government
# MEMORANDUM
NRL, Code 1201/1220, x70793/2240, MILLER@SECURITY

DATE: 8 Sep 00

FROM: Security Manager, Code 1220
TO: Head, Personnel Security and Visitor Control Section, Code 1224

SUBJ: DISSEMINATION OF FOREIGN DISCLOSURE INSTRUCTIONS

1. Confirming previous verbal instructions, when written foreign disclosure instructions are received from Navy International Programs Office or other appropriate authority, you are to ensure that copies of these instructions are provided as soon as possible to NRL points of contact for the visits in question.

John T. Miller

# Defense Advanced Research Projects Agency Comments

**DEFENSE ADVANCED RESEARCH PROJECTS AGENCY**
3701 NORTH FAIRFAX DRIVE
ARLINGTON, VA 22203-1714

SEP 2 6 2000

MEMORANDUM FOR ASSISTANT INSPECTOR GENERAL FOR AUDITING, DOD IG

SUBJECT: Audit Report on Foreign National Security Controls at DoD Research Laboratories (Project No. D1999LG-0034.03) (Formerly Project No. 9LG-5030.03)

This is in response to your recent "Draft of a Proposed Audit Report," subject as above. The Defense Advanced Research Projects Agency (DARPA) concurs with the recommendations (Attachment A), and we are actively taking corrective actions in three areas: continue to improve training for Office Directors, Deputy Directors, Assistant Directors for Program Management, Program Managers and Visitor Control Center personnel; complete the DARPA Security Manual and the associated Standard Operating Procedures and DARPA Instructions; and perform a system needs assessment for data base development.

Attachments A, B, C, D and E provide information concerning DARPA initiatives and status. I believe these initiatives have and will continue to make DARPA a more secure working environment.

DARPA takes exception to and requests revisions of certain conclusions and statements in the draft report. Some of the statements contained in the body of the report describe vulnerabilities that do not appear to be supported by the referenced data. As detailed in Attachment F, DARPA believes that certain conclusions stated in the report, related to the release of controlled unclassified and classified data, separate from the recommendations, inappropriately characterize the risk of inadvertent release of classified and controlled unclassified information, are potentially inflammatory, and are unnecessary to support the DoD IG recommendations.

DARPA maintains strong, multi-level controls on the release of classified information. DARPA technical personnel are aware of which information related to their programs is classified, are well versed in proper control of that information, and have ready assistance from the DARPA security organization when needed. With respect to classified foreign visits to DARPA for classified discussions, they are infrequent and subject to careful controls. On receipt from any source - the Defense Intelligence Agency (DIA), a DARPA Program Manager (PM), a U.S. company - of a request for a classified foreign visit, the DARPA Security and Intelligence Directorate coordinates with the proposed host to verify that the visitor has a *need to know* the particular classified information. The visit clearance request document, which forms the basis for the Foreign Disclosure Officer's approval of classified discussions, is the *only approved reference* if later verification of the visitor's clearance level becomes necessary.

With respect to unclassified foreign visits to DARPA for unclassified discussions, they are frequent. The DARPA host's function in most unclassified visits is to be in a "listening mode." Through continuing training and continuously available, Web-based reference materials, DARPA personnel, especially PMs, Technical Office Directors, and Deputy Directors

2

understand that in any situation in which the DARPA host has not received specific authorization for release of information, the host may discuss with foreign visitors <u>only</u> information that has been approved previously for public release. Stated more succinctly, the DARPA default with respect to information disclosure is that the host may disclose only information previously approved for public release. DARPA personnel are quite familiar with the sources for publicly released information, including the DARPA public Web site, approved public speeches, and certain open publications describing DARPA programs.

Moreover, for classified or unclassified visits, every visitor must check in at the Visitor Control Center (VCC). The VCC issues the visitor an escort-required badge, red for U.S. citizens and green for non-U.S. citizens and foreign nationals. The badge provides the DARPA host with a clear visual reminder as to whether a guest is a foreign national or not. For classified discussions with non-U.S. citizens or foreign nationals, the clearance level is established before the visit. Upon receipt of the visit request from DIA, the DARPA Security and Intelligence Directorate (SID) coordinates with the prospective host to establish the clearance level for discussions during the visit. SID then forwards a notification to the host approving the visit and the clearance level for discussions. The DARPA SIMS database is not used to verify a foreign visit clearance when issuing a badge.

DARPA is confident that its procedures - badges, training, default to publicly released information - provide clear and multi-faceted protection against inadvertent disclosure of sensitive unclassified or classified information.

Attachment G is a copy of a delegation of disclosure authority letter, and Attachment H is a copy of Chapter 10, "International Security," of the DARPA Security Manual. Attachments G and H are referred to in Attachment F.

We appreciate the opportunity to review the DoD IG draft report. If you have further questions regarding this response; please call our point of contact, Nancy Kassner, at (703) 696-2432.

F. L. Fernandez
Director

Attachments:
1. Tab A - DoD IG Recommendations with DARPA Actions Taken
2. Tab B - DARPA Training (Visitor Control Center, Program Managers and Assistant Directors, Program Management)
3. Tab C - Foreign Visit and Visitor Control Center Visitor Processing
4. Tab D - Security Information Management System Data Fields Descriptions
5. Tab E - International Security Enhancements (Gantt Chart)
6. Tab F - DARPA Comments on Certain Language Employed in the Draft Report
7. Tab G - Redelegation of Disclosure Authority
8. Tab H - Chapter 10, "International Security," DARPA Security Manual

\* Omitted because of length.  Copies will be provided on request.

DoD IG Recommendations

1. RECOMMENDATION: Director, DARPA develop local procedures to ensure foreign disclosure instructions from foreign visit approval authorities are disseminated to the program managers hosting foreign nationals.

ACTIONS TAKEN:
- Updating Security Manual (Gantt chart attached)
- Updating International Program's Standard Operating Procedures (SOP), December 31, 2000
- Updating Visitor Control Center (VCC) SOP, December 31, 2000
- Reminding DARPA personnel to utilize Web-based reference materials already available on the DARPA Intranet that provide security guidance to DARPA personnel for hosting a visit by foreign nationals
- Updating, improving and increasing the frequency of DARPA Security Training for Office Directors (ODs), Deputy Directors, Program Managers, Assistant Directors for Program Management (ADPMs), VCC personnel, and the international security function within the Security and Intelligence Directorate

2. RECOMMENDATION: Director, DARPA enforce and improve security procedures to ensure visits by foreign nationals are sufficiently documented to verify the citizenship and security clearance level of the foreign nationals.

ACTIONS TAKEN:
- Emphasizing Security Information Management System (SIMS) Training (August 16-18, 2000, for all VCC employees)
- Updating VCC SOP (December 31, 2000)
- Individual training to the ODs and ADPMs
- Initial security briefings to all newcomers
- DARPA Instruction on foreign visits

3. RECOMMENDATION: Director, DARPA prepare a manual providing specific procedures for the preparation of Visitor Control Center records with an explanation of each field to be completed to aid consistent record keeping.

ACTION TAKEN:
- Creating DARPA VCC worksheet with data fields notebook that will be part of the VCC SOP (August 16, 2000)

4. RECOMMENDATION: Develop SIMS database input methods that ensure the Defense Intelligence Agency visit approval letter is used as the primary source document for all information regarding official foreign national visitors.

ACTIONS TAKEN:
- Emphasizing SIMS Training (August 16-18, 2000, for all VCC employees)
- Database development (see attached Gantt chart)

Tab A

44

*Draft Audit: Foreign National Security Controls ...*
*Project No. D1999LG-0034.03*

DARPA Comments on Certain Language Employed in the Draft Report

------------------------------------------------------------------------------------------------

Draft Report, page ii **EXECUTIVE SUMMARY, Results**
*DoD IG: However, the Defense Advanced Research Projects Agency and the Naval Research Laboratory controls over the dissemination of foreign disclosures needed improvement. Specifically, for 208 of 270 official visits reviewed, the Defense Advanced Research Projects Agency and the Naval Research Laboratory did not disseminate foreign disclosure instructions to the program managers hosting foreign nationals. As a result, the Defense Advanced Research Projects Agency and the Naval Research Laboratory program managers were hosting foreign nationals on official visits unaware of national security foreign disclosure restraints and may have inadvertently released unauthorized technical information to other countries (finding A). The Military Department laboratories' approval processes for visits by foreign nationals were adequate (see Appendix C). However, the Defense Advanced Research Projects Agency security controls over the approval process for foreign national visitors were weak. Specifically, controls for granting building access for foreign national visitors representing U.S. entities required improvement. Also, the Defense Advanced Research Projects Agency database contained inconsistent and erroneous data. As a result, controls over the disclosure of controlled unclassified and classified information to foreign nationals were not effective and the Defense Advanced Research Projects Agency may have inadvertently disclosed controlled unclassified and classified information to other countries, including countries of concern, without authorization (finding B).*

DARPA COMMENT:

DARPA concurs with the DoD IG finding that the Visitor Control Center database reviewed by the DoD IG contained inconsistent and inaccurate data. However, this finding does not support the conclusion that *"As a result, controls over the disclosure of controlled unclassified and classified information to foreign nationals were not effective and the Defense Advanced Research Projects Agency may have inadvertently disclosed controlled unclassified and classified information to other countries, including countries of concern, without authorization (finding B)."* The DARPA Visitor Control Center database is not authorized for use by DARPA personnel as a source or reference to verify security clearances of foreign national visitors, either those representing a foreign entity or those representing a U.S. entity. Moreover, DARPA believes that the conclusion quoted above, and repeated in slightly different contexts elsewhere in the report, inappropriately inflates the actual risk of inadvertent release of DARPA classified and controlled unclassified information, is potentially inflammatory, and is unnecessary to support the DoD IG recommendations. In DARPA's exit briefing with the DoD IG review team, after extensive discussions of the DARPA foreign visitor control procedures, the DoD IG team agreed to delete the term "classified" information from these elements of their findings.

Foreign visits for unclassified discussions are frequent at DARPA. Foreign visits for classified discussions are very infrequent.

Attachment F                    Page 1 of 12 pages

<u>Classified</u>: Foreign visits to DARPA for classified discussions are infrequent and are subject to careful controls. On receipt from any source – the Defense Intelligence Agency (DIA), a DARPA Program Manager (PM), a U.S. company - of a request for a classified foreign visit, the DARPA Security and Intelligence Directorate (SID) coordinates with the proposed host to verify that the visitor has a *need to know* the particular classified information. The visit clearance request document, which forms the basis for the DARPA Security and Intelligence Directorate approval of classified discussions, is the *only approved reference* if later verification of the visitor's clearance level becomes necessary. DARPA does not authorize use of its Security Information Management System (SIMS) database for verification of clearance level.

  • For foreign visitors representing foreign entities, visit clearance requests are received via the Defense Intelligence Agency (DIA).

  • For foreign nationals representing U.S. entities, visit requests are received from the security offices of the U.S. entities.

In either case, DARPA receives and maintains on file certifications of the visitor's security clearance level from verified sources. While DARPA procedures include entry of the clearance level in the DARPA database, *the database is not an authorized source for verifying a foreign visitor's security clearance level.*

<u>Unclassified:</u> Foreign visits to DARPA for <u>unclassified</u> discussions are frequent. The DARPA host's function in most unclassified visits is to be in a "listening mode." Through continuing training and continuously available, Web-based reference materials, DARPA personnel, especially PMs and Technical Office Directors, understand that in any situation in which the DARPA host has not received specific authorization for release of information, the host may discuss with foreign visitors only information that has been approved previously for public release. Stated more succinctly, the DARPA default with respect to information disclosure is that the host may disclose only information previously approved for public release. DARPA personnel are quite familiar with the sources for publicly released information, including the DARPA public Web site, their own and the DARPA Director's approved public speeches, and certain open publications describing DARPA programs. In the terms of the DoD IG finding, an instance in which a DARPA host did not receive a copy of the DIA authorization for a foreign visit would result in the host disclosing less information than might have been authorized by DIA, not in release of more than authorized.

In addition, for classified or unclassified visits, to enter DARPA controlled spaces every visitor must check in at the Visitor Control Center (VCC). The VCC issues the visitor a badge with distinct attributes that identify nationality, by color; and security clearance level, if any, by a numeral designator. All foreign visitors to

Attachment F                    Page 2 of 12 pages

DARPA are escorted throughout their visits in DARPA spaces. Before issuing a badge with a security clearance designator to any visitor, foreign or not, VCC personnel must review the visit request document. They are not authorized to issue a badge with a clearance designator based upon review of the DARPA SIMS database.

The badges provide the DARPA host with a clear visual reminder as to whether a guest is a foreign national or not, and whether the visitor is authorized access to classified information.

Visits during which a DARPA host wishes to disclose controlled information are infrequent. In support of such a visit, the DARPA Security and Intelligence Directorate researches existing international agreements, drafts and coordinates approval of a delegation of disclosure authority letter (DDL) if necessary, and provides the prospective host with disclosure-related instructions. Like much correspondence with DARPA technical personnel, in view of their heavy travel schedules, this correspondence is often done via e-mail. Any useful information contained in DIA correspondence regarding the visit is repeated in the e-mail to the host.

DARPA is confident that its procedures – badges, training, the DARPA Security and Intelligence Directorate foreign disclosure process, default to publicly released information - provide clear and multi-faceted protection against inadvertent disclosure of controlled unclassified and classified information.

DARPA REQUEST:
DARPA requests that the DoD IG revise its report to delete the statement that *"... the Defense Advanced Research Projects Agency may have inadvertently disclosed controlled unclassified and classified information to other countries, including countries of concern, without authorization;"* or, DARPA requests that DoD IG identify the instances and the information that may have been disclosed, to allow DARPA to assess potential damage to the Agency or to DoD accruing from the improper disclosure.

Revised

------------------------------------------------------------------------------------------------------

Draft Report, page 2 ***Approval Authority for Foreign Nationals Representing Foreign Entities***
***DoD IG:*** *For official visits, that is, for meetings that involve foreign nationals representing foreign entities, a designated disclosure authority must approve foreign disclosure. The approval is documented in a visit authorization letter signed by a foreign disclosure officer. ... For the Defense Advanced Research Projects Agency (DARPA) in Arlington, Virginia, foreign disclosure authorization is centralized within the Defense Intelligence Agency.*

Attachment F          Page 3 of 12 pages

Revised

*Draft Audit: Foreign National Security Controls ...*
*Project No. D1999LG-0034.03*

DARPA COMMENT:

The Director, DARPA possesses delegated authority to approve foreign disclosures. The most recent delegation, signed by the Principal Deputy Under Secretary of Defense (Acquisition and Technology), dated May 17, 1994, delegates authority to disclose or deny, to foreign governments and international organizations, classified or unclassified, export controlled, scientific and technical information originated by or for DARPA. DARPA receives requests for official *foreign visits* from DIA. The "Visit Request Action" that DARPA receives from DIA requests that *DARPA state the disclosure authorization* for any controlled information to be disclosed if it approves the requested meeting, and *reminds DARPA of its responsibility* to protect information. DARPA SID then consults with the prospective DARPA visit host to review, and sometimes revise, the "purpose of visit" statement that appears on the DIA foreign visit request, and responds accordingly to DIA. DIA then sends a "Visit Request Approval," which repeats whatever disclosure approval DARPA has provided in its response to the DIA "Visit Request Action." For DARPA, foreign disclosure authorization is centralized in the DARPA Director's office, not within DIA.

DARPA REQUEST:

DARPA requests that the DoD IG recognize that the Director, DARPA possesses delegated authority to approve foreign disclosure, and consider clarifying the language of the report accordingly.

---------------------------------------------------------------------------------------

Draft Report, page 5 *A. Dissemination of Foreign Disclosure Instructions*
*DoD IG: However, DARPA and Navy Lab controls over the dissemination of foreign disclosure instructions needed improvement. Specifically, for 208 of 270 official visits reviewed, DARPA and the Navy Lab did not disseminate foreign disclosure instructions to the program managers hosting foreign nationals because DARPA and Navy instructions did not clearly state the procedures to be used for the dissemination of foreign disclosure instructions. As a result, DARPA and the Navy Lab program managers were hosting foreign nationals on official visits unaware of national security foreign disclosure restraints that pertained to the visitor's country of origin. Therefore, DARPA and the Navy Lab may have inadvertently released unauthorized technical information to other countries.*

DARPA COMMENT:

DARPA has and does provide foreign disclosure instructions to hosts of foreign visits. Through frequent training, e-mails, and continuously available Web-based reference materials, DARPA personnel who host foreign national visits, especially PMs and Technical Office Directors, are made aware of their responsibilities to protect information by this aggregation of means. They understand that classified information may be disclosed only after approval through DIA and a determination that the visitor has a need to know; they know the meaning in information disclosure terms of the badges issued to visitors by the VCC; and they know that the DARPA default is that, in the absence of specific disclosure authority, they are to disclose only publicly released information.

Attachment F                          Page 4 of 12 pages

*Draft Audit: Foreign National Security Controls ...*
*Project No. D1999LG-0034.03*

DARPA is confident that these procedures are adequate to prevent inadvertent release of unauthorized technical information to other countries.

DARPA REQUEST:
DARPA requests that DoD IG revise its report to delete the statement that *"... the Defense Advanced Research Projects Agency may have inadvertently disclosed controlled unclassified and classified information to other countries, including countries of concern, without authorization;"* or, DARPA requests that the DoD IG identify the instances and the information that may have been disclosed, to allow DARPA to assess potential damage to the Agency or to DoD accruing from the improper disclosure.

Revised

-------------------------------------------------------------------------------------

Draft Report, page 8
***DoD IG:*** *It is important that foreign disclosure instructions be disseminated because the foreign disclosure instructions in visit authorization letters refer to specific documents, such as delegation of disclosure authority letters, and are specific according to the country of the foreign national and the international agreement related to the purpose of the visit. Although the program manager hosting the foreign national is clearly the individual for whom the information is intended, many times the foreign disclosure instructions were not disseminated past the security office of the organization being visited.*

Draft Report, page 9 **DARPA and the Navy Lab**
***DoD IG:*** *DARPA did not provide foreign disclosure instructions from the Defense Intelligence Agency to the visit points of contact for about 60 percent of visits reviewed. The Navy Lab did not provide foreign disclosure instructions from the Navy International Programs Office to the visit points of contact for about 82 percent of visits reviewed. Table 2 shows the results of our review.*

Draft Report, page 9 *Foreign Disclosure at DARPA and the Navy Lab*
***DoD IG:*** *For more than half of the visits by foreign nationals representing foreign entities that we reviewed, the DARPA Security and Intelligence Directorate did not disseminate foreign disclosure instructions received from the Defense Intelligence Agency to the program managers hosting foreign national visitors. By reviewing the Security and Intelligence Directorate records of each visit by a foreign national representing a foreign entity, we determined that DARPA did not provide instructions to the visitor's host for 34 of 57 visits.*

Draft Report, page 9 *Foreign Disclosure at DARPA and the Navy Lab*
***DoD IG:*** *DARPA and the Navy Lab did not disseminate foreign disclosure instructions to program managers hosting foreign national visitors representing foreign entities because DARPA and Navy instructions do not clearly state the procedures to be used for the dissemination of foreign disclosure instructions.*

Attachment F                    Page 5 of 12 pages

DARPA COMMENT:

DARPA believes that DARPA staff hosting foreign visits had and have adequate foreign disclosure instructions, as a result of continuing training, continuously available, Web-based reference materials, and the DARPA policy that, in the absence of specific disclosure instructions, DARPA hosts are to disclose only information that has been publicly released. The visit requests that DARPA receives from DIA are standard-format Foreign Visit System (FVS) requests for a meeting. Each includes a generic "condition" statement applied by DIA (one of three, depending upon the level of classification – secret, confidential, or unclassified – that the embassy requests), a reference to DoD Directive 5230.11, and a statement that oral and visual disclosures are "subject to the conditions attached." As received by DARPA, no substantive "conditions" are attached, since DIA does not challenge or request clarification of an embassy's request. It is DARPA's responsibility to enter on the FVS request any substantive information that will inform the DARPA host of any useful information or restrictions applicable to the visit, other than the security classification level. After making appropriate entries, DARPA returns the revised FVS request to DIA, who will in turn pass it to the visitor's embassy. DARPA then transmits the same information to the prospective host, often by e-mail, since DARPA technical personnel are often on travel.

Most foreign visits to DARPA are unclassified, and most unclassified visits are approved authorizing the host to disclose only DARPA information already publicly released. In those cases, it is not DARPA's practice to provide the host with a copy of the DIA FVS request, because the DIA document does not contain information that is useful to the host.

In those infrequent cases when the DARPA host wishes to disclose controlled information, the DARPA Security and Intelligence Directorate and the prospective host coordinate in developing appropriate disclosure instructions. The DARPA Security and Intelligence Directorate drafts a delegation of disclosure authority letter and coordinates it for approval by the DARPA Director.

Through frequent training, e-mails, the DARPA Security and Intelligence Directorate foreign disclosure procedures, and continuously available Web-based reference materials, DARPA personnel, especially PMs and Technical Office Directors, are continually reminded that the DARPA default is: in the absence of specific disclosure authority, disclose only publicly available information. A warning to this effect is incorporated in e-mails provided to DARPA hosts in advance of official visits.

DARPA REQUEST:

DARPA requests that the DoD IG accept that DARPA procedures for visitor control and notification of hosts, when coupled with the DARPA default - that in the absence of specific disclosure instructions, hosts are to disclose only publicly

*Draft Audit: Foreign National Security Controls ...*
*Project No. D1999LG-0034.03*

released information – are sufficient to ensure protection from improper disclosure of classified information and unclassified controlled information.

---

Draft Report, page 10 *Official Visits by Foreign Nationals Representing Foreign Entities*

**DoD IG:** *For 34 of 57 visits by foreign nationals representing foreign entities, DARPA did not provide foreign disclosure instructions to the foreign visitor's host. The DARPA Security Manual does not provide policy or procedures for the dissemination of foreign disclosure limitations to the program managers who interact with or host visitors. The DARPA Security and Intelligence Directorate informal standard operating procedures for foreign visitors state that the Security and Intelligence Directorate will review the visit approval for disclosure issues and, if necessary, will review those issues with the program manager prior to the visit. However, since November 1999, a GS-13 Security Specialist position with supervisory duties over foreign disclosure duties had been vacant. As of June 2000, the position was still vacant.*

DARPA COMMENT:

DARPA concurs with the importance of having a security specialist for foreign disclosure control. At the time of the DoD IG review, the Government GS-14 position was being competitively advertised, and has since been filled, in August 2000.

DARPA REQUEST:

DARPA requests that the DoD IG revise the report to acknowledge that, while a GS-14 position was vacant, contractor personnel were performing the required functions, under the supervision and control of the Security and Intelligence Director.

---

Draft Report, page 10 *Unofficial Visits by Foreign Nationals Representing U.S. Entities*

**DoD IG:** *We selected a judgmental sample of 12 visits by foreign nationals representing U.S. entities from the Security Information Management System database. We selected visits by foreign nationals from countries of concern and visits by foreign nationals to discuss targeted technologies as identified by the Defense Security Service. For each of those selected visits, we interviewed the point of contact identified in the database. We verified that the visit took place, the dates of the visit, the information that was discussed, and what information had been released to the foreign nationals. Because DARPA did not require advance notice of unofficial visits (as discussed in finding B), foreign disclosure instructions were not prepared or disseminated to the program managers who interacted with or hosted the foreign national visitors.*

DARPA COMMENT:

DARPA believes that its security education program, information provided on the DARPA Intranet Web site, and e-mails provided to DARPA hosts in advance of unofficial foreign visits, provide appropriate information and instructions to its Office Directors, Deputy Office Directors and Program Managers regarding their

Attachment F                    Page 7 of 12 pages

risks and responsibilities with respect to protecting information during these
visits. Through frequent training, e-mails, and continuously available Web-based
reference materials, DARPA personnel, especially PMs, Technical Office
Directors, and Deputy Directors are made aware that, absent specific release
approval, they may discuss with foreign visitors only DARPA information that
previously has been approved for public release. They understand that the
DARPA default is, in the absence of specific disclosure authority, they are to
disclose only information that previously has been approved for public release.

DARPA REQUEST:
If the DoD IG determined that technical information was improperly disclosed
during the visits sampled, DARPA requests that the instances and disclosed
information be identified, to allow DARPA to assess any potential damage to the
Agency or to DoD. In the absence of a determination that technical information
was improperly disclosed, DARPA requests that the report acknowledge that the
DoD IG found no evidence of improper disclosures.

---

Draft Report, page 12 **Effect of Foreign Disclosure Control Weaknesses**
**DoD IG:** *DARPA and the Navy Lab may have inadvertently disclosed controlled*
*unclassified and classified information to foreign nationals without authorization.*
*Information on developing technologies available at DARPA and the Navy Lab is highly*
*sensitive. DARPA develops imaginative, high-risk research ideas that offer significant*
*technological impact. DARPA pursues technological concepts from the demonstration of*
*technical feasibility through the development of prototype systems.*

DARPA COMMENT:
None of the four examples given applies to DARPA.

DARPA REQUEST:
DARPA requests that the DoD IG remove DARPA from this paragraph.

---

Draft Report, page 17 **DARPA Compliance With Policies and Procedures**
**DoD IG:** *Table 3. "Results of DARPA Review"*
*DARPA did not comply with its policies and procedures governing visit requests by non-*
*DARPA personnel wishing to visit DARPA. The Visitor Control Center did not*
*consistently enforce security policies requiring advance notice for visits of non-DARPA*
*personnel. The DARPA Security Manual states that non-DARPA individuals must have*
*their security clearances and visit requests sent to the DARPA Visitor Control Center at*
*least two weeks in advance of an intended visit. However, the Security and Intelligence*
*Director stated that advance notice requirements were enforced only for meetings that*
*were expected to be classified. The Security and Intelligence Director stated that many*
*unclassified meetings took place everyday at DARPA where visit requests were not*
*required and no background data existed on the visitors.*

Attachment F                    Page 8 of 12 pages

DARPA COMMENT:

The Security and Intelligence Director recalls stating that many unclassified meetings took place at DARPA where visit requests were not provided in advance. All DARPA visitors are processed through the Visitor Control Center, which inquires as to the citizenship of each visitor and enters the information in its SIMS database. In this context, the statement "... no background data existed ..." is inaccurate, and the Security and Intelligence Director does not recall stating that background data does not exist.

Visitors to DARPA controlled spaces are processed through the DARPA Visitor Control Center, where background information on the visitor is entered in the DARPA SIMS database. Background information is entered into SIMS on foreign nationals who will be visiting with DARPA technical personnel. Foreign national visitors are issued a distinctively colored badge (green) that DARPA personnel understand identifies the visitors as foreign nationals, and the badge has no security clearance level numerical identifier, and DARPA personnel understand that this indicates that the foreign national visitor is not authorized access to any classified information.

DARPA has revised its security manual since the DoD IG visit, to differentiate the advance notice requirements for an official foreign visit that will involve disclosure of DARPA classified or controlled unclassified information, from the less stringent advance notice requirements for unofficial foreign visits during which the DARPA host will disclose only publicly released information. The revised manual no longer states that all foreign visit requests must be received two weeks in advance of a visit. Visits during which no disclosure will take place occur frequently at DARPA, they require no substantive instructions to the host, only a reminder to limit disclosure to publicly released information, and they do not require two-weeks advance notice. DARPA has revised its security manual to delete the two-week advance notification requirement with respect to these unofficial visits. The very infrequently occurring foreign visits during which the DARPA host wishes to disclose classified or controlled unclassified information still requires adequate advance notice.

As a matter of DARPA policy, little background information is entered on two categories of foreign national visitors: construction workers, and members of the janitorial staff. Because these workers are accompanied and monitored by a member of the VCC staff throughout each visit to DARPA spaces, their visits represent low risk of compromise of DARPA information or facilities. At the time of the DoD IG visit, DARPA entered no special code to differentiate these workers in the SIMS database. Thus while DARPA VCC personnel distinguish between these two kinds of visits, and could distinguish these entries in historical entries if requested, the DoD IG auditors had no basis for determining which SIMS entries were for these workers, and which were for foreign nationals visiting with DARPA scientists for discussions related to technology. If the DoD IG wishes, DARPA can identify these workers in any sample of historical data

*Draft Audit: Foreign National Security Controls ...*
*Project No. D1999LG-0034.03*

from its SIMS database. To make its database more auditor-accessible, DARPA
has begun coding entries so that the distinction will be more apparent to
reviewers.

DARPA REQUEST:
  DARPA requests that the DoD IG revise the report to delete the attribution to the
  Security and Intelligence Director of a statement that "... no background data
  existed ..." on foreign visitors.

---

Draft Report, page 18 *Effect of Foreign Disclosure Control Weaknesses at DARPA*
*DoD IG: The information on developing technology available at DARPA is highly*
*sensitive. Controls over the disclosure of controlled unclassified and classified*
*information to foreign nationals at DARPA were not effective. Because DARPA did not*
*require advance notice for meetings that were expected to be unclassified, foreign*
*nationals unexpectedly attended several meetings. When we interviewed program*
*managers who had hosted foreign nationals representing U.S. entities, 4 of 12 program*
*managers interviewed stated they were unaware until the meetings took place that they*
*were hosting foreign nationals at the meetings in question. The four foreign nationals*
*were from three countries of concern: China, Israel, and Syria.*

DARPA COMMENT:
  DARPA concurs with the DoD IG Recommendation that DARPA enforce and
  improve procedures to ensure visits by foreign nationals representing U.S. entities
  are sufficiently documented to verify the citizenship of the visitors. DARPA has
  stated that it has implemented improvements in notifying DARPA hosts of the
  citizenship of their visitors. The implementation has been done in a manner to
  provide an improved audit trail for third-party reviewers.

  In three of the four cases cited by the DoD IG, the DARPA host recognized
  before information exchange took place that one or more guests were foreign
  nationals, and acted appropriately. DARPA is confident that its security
  education program, Web-based reference materials, and e-mail notification
  process are working. DARPA's first line of defense against improper disclosure
  of information is the education of its professional personnel as to their
  responsibilities to protect information. DARPA personnel who host foreign
  visitors are continually drilled that the DARPA default position is that, in the
  absence of specific authority to release information, they may disclose to foreign
  visitors only information that previously has been approved for public disclosure.

  In each of the four cases cited by the DoD IG, the DARPA host stated that the
  information discussed was unclassified and non-sensitive. This calls into question
  the statement in the report that "Controls over the disclosure of controlled
  unclassified and classified information to foreign nationals at DARPA were not
  effective." In none of the examples cited by the DoD IG was controlled
  unclassified or classified information improperly disclosed; without examples of
  improper disclosure, one would conclude that controls were effective.

Attachment F                    Page 10 of 12 pages

*Draft Audit: Foreign National Security Controls ...*
*Project No. D1999LG-0034.03*

**DARPA REQUEST:**

DARPA requests that the DoD IG revise its statement that controls over the
disclosure of controlled unclassified or classified information were not effective.

---------------------------------------------------------------------------------------------------------

Draft Report, page 19
***DoD IG:*** *Because DARPA had* <u>erroneous</u> *records ... (emphasis added)*

Draft Report, page 20
***DoD IG:*** *... The inconsistent and* <u>erroneous</u> *documentation of visits and visitors could
result in ... program managers believing that individuals had access to higher
classifications of information than the individuals had actually been cleared for, thereby
causing program managers to inadvertently* <u>release unauthorized classified data</u> *to
foreign nationals. (emphases added)*

**DARPA COMMENT:**

DARPA does not discount the importance of ensuring accuracy of database
entries. However, DARPA takes exception to the extrapolation of a single
observed instance of an inaccurate entry to statements of "erroneous"
documentation, and to the statement that this (entry) could result in inadvertent
release of unauthorized classified information. DARPA has taken appropriate
measures that greatly improve the accuracy of documentation of foreign visits in
its database. However, DARPA is confident that the chance that an entry of an
inaccurate clearance level in the DARPA database would result in inadvertent
release of classified information is remote. Most foreign visits to DARPA,
including the example cited by the DoD IG, are for unclassified discussions.
Foreign visits for classified discussions are not common. For such visits, the visit
clearance document, not the DARPA database, forms the basis for the DARPA
Security and Intelligence Directorate's approval of classified discussions. The
SIMS database that the DoD IG reviewed is not accessible to DARPA scientific
and management personnel, and is not an authorized source of verifying security
clearances of foreign visitors. Hosts wishing to verify the clearance of a foreign
visitor are referred to the DARPA Security and Intelligence Directorate, which
reviews the visit clearance source document, not the database, for confirmation.
DARPA has followed up with hosts of foreign visits, and has found no evidence
that hosts of foreign visits considered the SIMS database to be an appropriate
source for verifying a foreign visitor's clearance, or requested such information
for verification purposes from the VCC personnel who access the SIMS database.
DARPA personnel are aware that, in the absence of specific authority to disclose
information, they may discuss with foreign visitors only information that
previously has been approved for public release. DARPA has found no evidence
that classified information was improperly disclosed to foreign nationals as a
result of these erroneous database entries.

Attachment F                    Page 11 of 12 pages

*Draft Audit: Foreign National Security Controls ...*
*Project No. D1999LG-0034.03*

DARPA REQUEST:

DARPA requests that the DoD IG review the report, to ensure that the report statements recognize that no examples were found of DARPA inadvertently disclosing unclassified controlled data or classified data to foreign nationals; and that the SIMS database is not the record employed by DARPA to notify hosts of the clearance levels of foreign visitors. DARPA further requests that the DoD IG revise the language of the report to state that it found inaccurate records, rather than erroneous records.

Attachment F                          Page 12 of 12 pages

# Audit Team Members

The Readiness and Logistics Support Directorate, Office of the Assistant Inspector General for Auditing, DoD, prepared this report. Personnel of the Office of the Inspector General, DoD, who contributed to the report are listed below.

Shelton R. Young
Evelyn R. Klemstine
Timothy E. Moore
Jane T. Thomas
Julie C. Kienitz
David L. Leising
Frank J. Kelly
Christine M. McIsaac
Jessica K. Sekhon

# INTERNET DOCUMENT INFORMATION FORM

**A . Report Title:** Foreign National Security Controls at DoD Research Laboratories

**B. DATE Report Downloaded From the Internet:** 11/01/00

**C. Report's Point of Contact: (Name, Organization, Address, Office Symbol, & Ph #):** OAIG-AUD (ATTN: AFTS Audit Suggestions)
Inspector General, Department of Defense
400 Army Navy Drive (Room 801)
Arlington, VA 22202-2884

**D. Currently Applicable Classification Level:** Unclassified

**E. Distribution Statement A:** Approved for Public Release

**F. The foregoing information was compiled and provided by:**
DTIC-OCA, Initials: __VM__ Preparation Date 11/01/00

The foregoing information should exactly correspond to the Title, Report Number, and the Date on the accompanying report document. If there are mismatches, or other questions, contact the above OCA Representative for resolution.